

**Pt. 504, App. E**

are requested to provide the following account information pertaining to (identify customer);

(Describe the specific records to be examined)

The Army has no authority to issue an administrative summons or subpoena for access to these financial records which are required for (describe the nature or purpose of the inquiry).

A copy of this request was (personally served upon or mailed to) the subject on (date) who has (10 or 14) days in which to challenge this request by filing an application in an appropriate United States district court if the subject desires to do so.

Upon expiration of the above mentioned time period and in the absence of any filing or challenge by the subject, you will be furnished a certification certifying in writing that the applicable provisions of the Act have been complied with prior to obtaining the requested records. Upon your receipt of a Certificate of Compliance with the Right to Financial Privacy Act of 1978, you will be relieved of any possible liability to the subject in connection with the disclosure of the requested financial records.

(Official Signature Block)

**APPENDIX E TO PART 504—CUSTOMER NOTICE OF FORMAL WRITTEN REQUEST—SAMPLE FORMAT**

(Official Letterhead)

(Date) \_\_\_\_\_  
Mr./Ms. \_\_\_\_\_,  
1500 N. Main Street, Washington, DC 20314.

Dear Mr./Ms. \_\_\_\_\_: Information or records concerning your transactions held by the financial institution named in the attached request are being sought by the (agency/department) in accordance with the Right to Financial Privacy Act of 1978, section 3401 et seq., Title 12, United States Code, and Army Regulation 190-6, for the following purpose(s):

(List the purpose(s))

If you desire that such records or information not be made available, you must do the following:

a. Fill out the accompanying motion paper and sworn statement or write one of your own—

(1) Stating that you are the customer whose records are being requested by the Government.

(2) Giving the reasons you believe that the records are not relevant or any other legal basis for objecting to the release of the records.

b. File the motion and statement by mailing or delivering them to the clerk of any

**32 CFR Ch. V (7-1-02 Edition)**

one of the following United States District Courts:

(List applicable courts)

c. Mail or deliver a copy of your motion and statement to the requesting authority: (give title and address).

d. Be prepared to come to court and present your position in further detail.

You do not need to have a lawyer, although you may wish to employ one to represent you and protect your rights.

If you do not follow the above procedures, upon the expiration of (10 days from the date of personal service) (14 days from the date of mailing) of this notice, the records or information requested therein may be made available.

These records may be transferred to other Government authorities for legitimate law enforcement inquiries, in which event you will be notified after the transfer if such transfer is made.

3 Inclosures (see para—)

(Signature) \_\_\_\_\_

**PART 505—THE ARMY PRIVACY PROGRAM**

Sec.

505.1 General information.

505.2 Individual rights of access and amendment.

505.3 Disclosure of personal information to other agencies and third parties.

505.4 Record-keeping requirements under the Privacy Act.

505.5 Exemptions.

APPENDIX A TO PART 505—EXAMPLE OF SYSTEM OF RECORDS NOTICE

APPENDIX B TO PART 505—EXAMPLE OF REPORT FOR NEW SYSTEM OF RECORDS

APPENDIX C TO PART 505—PROVISIONS OF THE PRIVACY ACT FROM WHICH A GENERAL OR SPECIFIC EXEMPTION MAY BE CLAIMED

APPENDIX D TO PART 505—GLOSSARY OF TERMS

AUTHORITY: Pub. L. 93-579, 88 Stat. 1896 (5 U.S.C. 552a).

SOURCE: 50 FR 42164, Oct. 18, 1985, unless otherwise noted.

**§ 505.1 General information.**

(a) *Purpose.* This regulation sets forth policies and procedures that govern personal information kept by the Department of the Army in systems of records.

(b) *References*—(1) *Required publications.* (i) AR 195-2, Criminal Investigation Activities. (Cited in § 505.2(j))

## Department of the Army, DoD

## § 505.1

(ii) AR 340-17, Release of Information and Records from Army Files. (Cited in §§ 505.2(h) and 505.4(d))

(iii) AR 430-21-8, The Army Privacy Program; System Notices and Exemption Rules for Civilian Personnel Functions. (Cited in § 505.2(i))

(iv) AR 380-380, Automated System Security. (Cited in § 505.4(d) and (f))

(2) *Related publications.* (A related publication is merely a source of additional information. The user does not have to read it to understand this regulation.)

(i) DOD Directive 5400.11, DOD Privacy Program.

(ii) DOD Regulation 5400.11-R, DOD Privacy Program.

(iii) Treasury Fiscal Requirements Manual. This publication can be obtained from The Treasury Department, 15th and Pennsylvania Ave., NW, Washington, DC 20220

(c) *Explanation of abbreviations and terms.* Abbreviations and special terms used in this regulation are explained in the glossary.

(d) *Responsibilities.* (1) The Director of Information Systems for Command, Control, Communications, and Computers (DISC4) is responsible for issuing policy and guidance for the Army Privacy Program in consultation with the Army General Counsel.

(2) The Commander, U.S. Army Information Systems Command is responsible for developing policy for and executing the Privacy Act Program under the policy and guidance of the DISC4.

(3) Heads of Joint Service agencies or commands for which the Army is the Executive Agent, or otherwise has responsibility for providing fiscal, logistical, or administrative support, will adhere to the policies and procedures in this regulation.

(4) Commander, Army and Air Force Exchange Service (AAFES), is responsible for the supervision and execution of the privacy program within that command pursuant to this regulation.

(e) *Policy.* Army Policy concerning the privacy rights of individuals and the Army's responsibilities for compliance with operational requirements established by the Privacy Act are as follows:

(1) Protect, as required by the Privacy Act of 1974 (5 U.S.C. 552a), as

amended, the privacy of individuals from unwarranted intrusion. Individuals covered by this protection are living citizens of the United States and aliens lawfully admitted for permanent residence.

(2) Collect only the personal information about an individual that is legally authorized and necessary to support Army operations. Disclose this information only as authorized by the Privacy Act and this regulation.

(3) Keep only personal information that is timely, accurate, complete, and relevant to the purpose for which it was collected.

(4) Safeguard personal information to prevent unauthorized use, access, disclosure, alteration, or destruction.

(5) Let individuals know what records the Army keeps on them and let them review or get copies of these records, subject to exemptions authorized by law and approved by the Secretary of the Army. (See § 505.5.)

(6) Permit individuals to amend records about themselves contained in Army systems of records, which they can prove are factually in error, not up-to-date, not complete, or not relevant.

(7) Allow individuals to ask for an administrative review or decisions that deny them access to or the right to amend their records.

(8) Maintain only information about an individual that is relevant and necessary for Army purposes required to be accomplished by statute or Executive Order.

(9) Act on all requests promptly, accurately, and fairly.

(f) *Authority.* The Privacy Act of 1974 (5 U.S.C. 552a), as amended, is the statutory basis for the Army Privacy Program. Within the Department of Defense, the Act is implemented by DOD Directive 5400.11 and DOD 5400.11-R. The Act Assigns—

(1) Overall Government-wide responsibilities for implementation to the Office of Management and Budget.

(2) Specific responsibilities to the Office of Personnel Management and the General Services Administration.

(g) *Access and Amendment Refusal Authority (AARA).* Each Access and Amendment Refusal Authority (AARA) is responsible for action on requests for

access to, or amendment of, records referred to them under this part. The officials listed below are the only AARA for records in their authority. Authority may be delegated to an officer or subordinate commander. All delegations must be in writing. If an AARA's delegate denies access or amendment, the delegate must clearly state that he or she is acting on behalf of the AARA and identify the AARA by name and position in the written response to the requester. Denial of access or amendment by an AARA's delegate must have appropriate legal review. Delegations will not be made below the colonel (06) or GS/GM-15 level. Such delegations must not slow Privacy actions. AARAs will send the names, offices, telephone numbers of their delegates to the Director of Information Systems for Command, Control, Communications and Computers, Headquarters, Department of the Army, ATTN: SAIS-IDP, Washington, DC 20310-0107; and the Department of the Army Privacy Review Board, Crystal Square 1, Suite 201, 1725 Jefferson Davis Highway, Arlington, VA 22202.

(1) The Administrative Assistant to the Secretary of the Army (AASA) for records of the Secretariat and its serviced activities, to include the personnel records maintained by the General Officer Management Office, personnel records pertaining to Senior Executive Service personnel serviced by the Office of the Secretary of the Army (OSA), and Equal Employment Opportunity (EEO) records from offices serviced by the OSA. The AASA will also serve as AARA for those records requiring the personal attention of the Secretary of the Army.

(2) The Inspector General (TIG) for TIG investigative records.

(3) The president or executive secretary of boards, councils, and similar bodies established by the Department of the Army to consider personnel matters, including the Army Board of Correction of Military Appeals, for records under their purview.

(4) The Deputy Chief of Staff for Personnel (DCSPER) for records of active and former non-appropriated fund employees (except those in the Army and Air Force Exchange Service), alcohol and drug abuse treatment records, be-

havioral science records, recruiting, Armed Services Vocational Aptitude Battery (ASVAB), equal opportunity, Junior Reserve Officers' Training Corps (ROTC), Senior ROTC Instructor, military academy cadet, selection, promotion, and reduction boards; special review boards; professional staff informational records; and entrance processing records (when records pertain to those not entering active duty).

(5) The Deputy Chief of Staff for Operations and Plans (DCSOPS) for military police records and reports and prisoner confinement and correctional records.

(6) Chief of Engineers (COE) for records pertaining to civil work (including litigation), military construction, engineer procurement, other engineering matters not under the purview of another AARA, ecology, and contractor qualifications.

(7) The Surgeon General (TSG) for medical records, except properly part of the Official Personnel Folder (OPM/GOVT-1 system of records).

(8) Chief of Chaplains (CCH) for ecclesiastical records.

(9) The Judge Advocate General (TJAG) for legal records under TJAG responsibility.

(10) Chief, National Guard Bureau (NGB) for personnel records of the Army National Guard.

(11) Chief, Army Reserve (CAR) for personnel records of Army retired, separated and reserve military personnel members.

(12) Commander, United States Army Material Command (USAMC) for records of Army contractor personnel of the Army Material Command.

(13) Commander, United States Army Criminal Investigation Command (USACIDC) for criminal investigation reports and military police reports included therein.

(14) Commander, United States Total Army Personnel Command (PERSCOM) for personnel and personnel related records of Army members on active duty and current Federal appropriated fund civilian employees. (Requests from former civilian employees to amend a record in any OPM system of records such as the Official Personnel Folder should be sent to the Office of

## Department of the Army, DoD

## § 505.2

Personnel Management, Assistant Director for Workforce Information, Compliance and Investigations Group, 1900 E Street, NW., Washington, DC 20415-0001.

(15) Commander, U.S. Army Community and Family Support Center (USACFSC) for records relating to morale, welfare and recreation activities; community life programs; family action programs, retired activities, club management, Army emergency relief, consumer protection, retiree survival benefits, and records dealing with Department of the Army relationships and social security veteran's affairs, United Service Organizations, U.S. Soldiers' and Airmen's home and American Red Cross.

(16) Commander, U.S. Army Intelligence and Security Command (INSCOM) for intelligence, investigative and security records; foreign scientific and technological information; intelligence training, mapping and geodesy information; ground surveillance records; intelligence threat assessments; and missile intelligence data relating to tactical land warfare systems.

(17) Commander, Army and Air Force Exchange Service (AAFES) for records pertaining to employees, patrons, and other matters which are the responsibility of the Exchange Service.

(18) Commander, Military Traffic Management Command (MTMC) for transportation records.

(19) Director of Army Safety for safety records.

(20) Commander, U.S. Army Information Systems Command (USAISC) for records which do not fall within the functional area of another AARA.

(h) *Department of the Army Privacy Review Board.* The Department of the Army Privacy Review Board acts on behalf of the Secretary of the Army in deciding appeals from refusal of the appropriate AARAs to amend records. Board membership is comprised of the AASA, the Commander, USAISC, Pentagon, and TJAG, or their representatives. The AARA may serve as a non-voting member when the Board considers matters in the AARA's area of functional specialization. The Commander, USAISC, Pentagon, chairs the Board and provides the recording secretary.

(i) *Privacy Official.* (1) Heads of Army Staff agencies and commanders of major Army commands and subordinate commands and activities will designate a privacy official who will serve as a staff adviser on privacy matters. This function will not be assigned below battalion level.

(2) The privacy official will ensure that (i) requests are processed promptly and responsively, (ii) records subject to the Privacy Act in his/her command/agency are described properly by a published system notice, (iii) privacy statements are included on forms and questionnaires that seek personnel information from an individual, and (iv) procedures are in place to meet reporting requirements.

[50 FR 42164, Oct. 18, 1985, as amended at 58 FR 51012, Sept. 30, 1993]

### § 505.2 Individual rights of access and amendment.

(a) *Access under the Privacy Act.* Upon a written or oral request, an individual or his/her designated agent or legal guardian will be granted access to a record pertaining to that individual, maintained in a system of records, unless the record is subject to an exemption and the system manager has invoked the exemption (see § 505.5), or the record is information compiled in reasonable anticipation of a civil action or proceeding. The requester does not have to state a reason or otherwise justify the need to gain access. Nor can an individual be denied access solely because he/she refused to provide his/her Social Security Number unless the Social Security Number was required for access by statute or regulation adopted prior to January 1, 1975. The request should be submitted to the custodian of the record.

(b) *Notifying the individual.* The custodian of the record will acknowledge requests for access within 10 work days of receipt. Records will be provided within 30 days, excluding Saturdays, Sundays, and legal public holidays.

(c) *Relationship between the Privacy Act and the Freedom of Information Act.* A Privacy Act request for access to records should be processed also as a Freedom of Information Act request. If

## § 505.2

## 32 CFR Ch. V (7–1–02 Edition)

all or any portion of the requested material is to be denied, it must be considered under the substantive provisions of both the Privacy Act and the Freedom of Information Act. Any withholding of information must be justified by asserting a legally applicable exemption in each Act.

(d) *Functional requests.* If an individual asks for his/her record and does not cite, or reasonably imply, either the Privacy Act or the Freedom of Information Act, and another prescribing directive authorizes release, the records should be released under that directive. Examples of functional requests are military members asking to see their Military Personnel Records Jacket, or civilian employees asking to see their Official Personnel Folder.

(e) *Medical records.* If it is determined that releasing medical information to the data subject could have an adverse affect on the mental or physical health of that individual, the requester should be asked to name a physician to receive the record. The data subject's failure to designate a physician is not a denial under the Privacy Act and cannot be appealed.

(f) *Third party information.* Third party information pertaining to the data subject may not be deleted from a record when the data subject requests access to the record unless there is an established exemption (see § 505.5(d)). However, personal data such as SSN and home address of third parties in the data subject's record normally do not pertain to the data subject and therefore may be withheld. Information about the relationship between the data subject and the third party would normally be disclosed as pertaining to the data subject.

(g) *Referral of records.* Requests for access to Army systems of records containing records that originated with other DOD Components or Federal agencies which claimed exemptions for them will be coordinated with or referred to the originator for release determination. The requester will be notified of the referral.

(h) *Fees.* Requesters will be charged only for the reproduction of requested documents. Normally, there will be no charge for the first copy of a record provided to the individual whose record

it is. Thereafter, fees will be computed as set forth in AR 340–17.

(i) *Denial of access.* (1) The only officials authorized to deny a request from a data subject for records in a system of records pertaining to that individual are the appropriate Access and Amendment Refusal Authorities (see § 505.1(f)), or the Secretary of the Army, acting through the General Counsel. Denial is appropriate only if the record:

(i) Was compiled in reasonable anticipation of a civil action or proceeding, or

(ii) Is properly exempted by the Secretary of the Army from the disclosure provisions of the Privacy Act (see § 505.5), there is a legitimate governmental purpose for invoking the exemption, and it is not required to be disclosed under the Freedom of Information Act.

(2) Requests for records recommended to be denied will be forwarded to the appropriate AARA within 5 work days of receipt, together with the request, disputed records, and justification for withholding. The requester will be notified of the referral.

(3) Within the 30 work day period (see § 505.2(b)), the AARA will give the following information to the requester in writing if the decision is to deny the request for access:

(i) Official's name, position title, and business address;

(ii) Date of the denial;

(iii) Reasons for the denial, including citation of appropriate section(s) of the Privacy Act and this regulation;

(iv) The opportunity for further review of the denial by the General Counsel, Office, Secretary of the Army, The Pentagon, Washington, DC 20310, through the AARA within 60 calendar days. (For denials made by the Army when the record is maintained in one of OPM's government-wide systems of records, notices for which are described at appendix B, AR 340–21–8, an individual's request for further review must be addressed to the Assistant Director for Agency Compliance and Evaluation, Office of Personnel Management, 1900 E Street NW., Washington, DC 20415–0001.)

(j) *Amendment of records.* (1) Individuals may request the amendment of

## Department of the Army, DoD

## § 505.2

their records, in writing, when such records are believed to be inaccurate as a matter of fact rather than judgment, irrelevant, untimely, or incomplete.

(2) The amendment procedures are not intended to permit challenge to a record that records an event that actually occurred nor are they designed to permit collateral attack upon that which has been the subject of a judicial or quasi-judicial action. Consideration of request for an amendment would be appropriate if it can be shown that circumstances leading up to the event that is recorded on the document were challenged through administrative procedures and found to be inaccurately described, that the document is not identical to the individual's copy, or that the document was not constructed in accordance with the applicable recordkeeping requirements prescribed. For example, the amendment provisions do not allow an individual to challenge the merits of an adverse action. However, if the form that documents the adverse action contains an error on the fact of the record (e.g., the individual's name is misspelled, an improper date of birth or SSN was recorded), the amendment procedures may be used to request correction of the record.

(3) US Army Criminal Investigations Command reports of investigation (records in system notices AO501.08e Informant Register, AO508.11b Criminal Information Reports and Cross Index Card Files, and AO508.25a Index to Criminal Investigative Case Files) have been exempted from the amendment provisions of the Privacy Act. Requests to amend these reports will be considered under AR 195-2 by the Commander, US Army Criminal Investigations Command, action by the Commander, US Army Criminal Investigation Command will constitute final action on behalf of the Secretary of the Army under that regulation.

(4) Records accessioned into the National Archives are exempted from the Privacy Act provision allowing individuals to request amendment of records. Most provisions of the Privacy Act apply only to those systems of records which are under the legal control of the originating agency; e.g., an agen-

cy's current operating files or records stored at a Federal records center.

(k) *Procedures.* (1) Requests to amend a record should be addressed to the custodian or system manager of that record. The request must reasonably describe the record to be amended and the changes sought (i.e., deletion, addition, amendment). The burden of proof rests with the requester; therefore, the alteration of evidence presented to courts, boards, and other official proceedings is not permitted. (An individual acting for the requester must supply a written consent signed by the requester.)

(2) The custodian or system manager will acknowledge the request within 10 work days and make final response within 30 work days.

(3) The record for which amendment is sought must be reviewed by the proper system manager or custodian for accuracy, relevance, timeliness, and completeness so as to assure fairness to the individual in any determination made about that individual on the basis of that record.

(4) If the amendment is proper, the custodian or system manager will physically amend the record by adding or deleting information, or destroying the record or a portion of it, and notify the requester of such action.

(5) If the amendment is not justified, the request and all relevant documents, including the reasons for not amending, will be forwarded to the appropriate AARA within 5 work days and the requester so notified.

(6) The AARA, on the basis of the evidence, either will amend the record and notify the requester and the custodian of that decision, or will deny the request and inform the requester:

- (i) Of reasons for not amending; and
- (ii) Of his/her right to seek further review by the DA Privacy Review Board (through the AARA).

(7) On receipt of an appeal from a denial to amend, the AARA will append any additional records or background information that substantiates the refusal or renders the case complete and, within 5 work days of receipt, forward the appeal to the DA Privacy Review Board.

(8) The DA Privacy Review Board, on behalf of the Secretary of the Army,

### § 505.3

### 32 CFR Ch. V (7-1-02 Edition)

will complete action on a request for further review within 30 work days of its receipt by the AARA. The General Counsel may authorize an additional 30 days when unusual circumstances and good cause so warrant. The Board may seek additional information, including the appellant's official file, if deemed relevant and necessary to deciding the appeal.

(i) If the Board determines that amendment is justified, it will amend the record and notify the requester, the AARA, the custodian of the record, and any prior recipients of the record.

(ii) If the Board denies the request, it will obtain the General Counsel's concurrence. Response to the appellant will include reasons for denial and the appellant's right to file a statement of disagreement with the Board's action and to seek judicial review of the Army's refusal to amend.

(9) Statements of disagreement will be an integral part of the record to which it pertains so the fact that the record is disputed is apparent to anyone who may have access to, use of, or need to disclose from it. The disclosing authority may include a brief summary of the Board's reasons for not amending the disputed record. The summary will be limited to the reasons stated to the individual by the Board.

(1) *Privacy case files.* Whenever an individual submits a Privacy Act request, a case file will be established; see system notice AO240.01DAAG. In no instance will the individual's request and Army actions thereon be included in the individual's personnel file. The case file will comprise the request for access/amendment, grants, refusals, coordination action, and related papers. This file will not be used to make any determinations about the individuals.

#### **§ 505.3 Disclosure of personal information to other agencies and third parties.**

(a) *Disclosure without consent.* The Army is prohibited from disclosing a record from a system of records without obtaining the prior written consent of the data subject, except when disclosure is:

(1) To those officers and employees of the Department of Defense who have a

need for the record in the performance of their duties;

(2) Required under the Freedom of Information Act (see § 505.3(c) for information normally releasable);

(3) Permitted by a routine use that has been published in the FEDERAL REGISTER;

(4) To the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to title 13 of the United States Code;

(5) To a recipient who has provided the Army with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

(6) To the National Archives of the United States as a record that has sufficient historical or other value to warrant its continued preservation by the U.S. Government, or for determination of such value by the Administrator of the General Services Administration (GSA), or designee. (Records sent to Federal Records Centers for storage remain under Army control; these transfers are not disclosures and do not therefore need an accounting.)

(7) To another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the Army element which maintains the record. The request must specify the particular portion desired and the law enforcement activity for which the record is sought;

(8) To a person pursuant to a showing of compelling circumstances affecting the health and safety of an individual. Upon such disclosure, notification will be transmitted to the last known address of such individual;

(9) To either House of Congress, or to a committee or subcommittee to the extent that the subject matter falls within the jurisdiction of the committee or subcommittee;

(10) To the Comptroller General, or any authorized representative in the

## Department of the Army, DoD

## § 505.3

course of the performance of the duties of the General Accounting Office;

(11) Pursuant to the order signed by a judge of a court of competent jurisdiction. (Reasonable efforts must be made to notify the individual if the legal process is a matter of public record); or

(12) To a consumer reporting agency in accordance with section 3(d) of the Federal Claims Collection Act of 1966 (originally codified at 31 U.S.C. 952(d); recodified at 31 U.S.C. 3711(f), the name, address, SSN, other information identifying the individual; amount, status, and history of the claim, and the agency or program under which the case arose may be disclosed in this instance.

(b) *Blanket routine use disclosures.* In addition to the routine uses in each system notice, the following blanket routine uses apply to all records from systems of records maintained by the Army except those which state otherwise.

(1) *Law enforcement.* Relevant records maintained to carry out Army functions may be referred to Federal, State, local, or foreign law enforcement agencies if the record indicates a violation or potential violation of law. The agency to which the records are referred must be the appropriate agency charged with the responsibility of investigating or prosecuting the violation or charges, with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

(2) *Disclosure when requesting information.* A record may be disclosed to a Federal, State, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, to obtain information relevant to an Army decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

(3) *Disclosure of requested information.* If the information is relevant and necessary to the requesting agency's decision, a record may be disclosed to a Federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance

of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

(4) *Congressional inquiries.* Disclosure from a system of records maintained by the Army may be made to a Congressional office from the record of an individual in response to an inquiry from the Congressional office made at the request of that individual.

(5) *Private relief legislation.* Relevant information in all systems of records of the Department of Defense published on or before August 22, 1975, will be disclosed to the Office of Management and Budget (OMB) review of private relief legislation as set forth in OMB Circular A-19 at any stage of the legislative coordination and clearance process.

(6) *Disclosures required by international agreements.* A record may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities. These disclosures are in compliance with requirements imposed by, or to claim rights conferred in, international agreements and arrangements including those regulating the stationing and status in foreign countries of DOD military and civilian personnel.

(7) *Disclosure to State and local taxing authorities.* Any information normally contained in Internal Revenue Service Form W-2 which is maintained in a record from a system of records of the Army may be disclosed to State and local taxing authorities with which the Secretary of the Treasury has entered into agreements under 5 U.S.C., sections 5516, 5517, and 5520 only to those State and local taxing authorities for which an employee or military member is or was subject to tax regardless of whether tax is or was withheld. This routine use complies with Treasury Fiscal Requirements Manual, Sec. 5060.

(8) *Disclosures to the Office of Personnel Management.* A record may be disclosed to the Office of Personnel Management (OPM) concerning information on pay and leave, benefits, retirement deduction, and any other information necessary for the OPM to



### § 505.3

### 32 CFR Ch. V (7–1–02 Edition)

carry out its legally authorized government-wide personnel management functions and studies.

(9) *Disclosure to National Archives and Records Administration.* A record may be disclosed to the National Archives and Records Administration in records management inspections conducted under authority of title 44 U.S.C., sections 2904 and 2906.

(10) *Disclosure to the Department of Justice for Litigation.* A record may be disclosed as a routine use to any component of the Department of Justice, when—

(i) The agency, or any component thereof, or

(ii) Any employee of the agency in his or her official capacity, or

(iii) Any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee, or

(iv) The United States, where the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice is deemed by the agency to be relevant and necessary to the litigation, provided, however, that in each case, the agency determines that disclosure of the records to the Department of Justice is a use of the information contained in the records that is compatible with the purpose for which it is collected.

(11) *Disclosure for Agency use in Litigation.* A record may be disclosed in a proceeding before a court or adjudicative body before which the agency is authorized to appear, when—

(i) The agency, or any component thereof, or

(ii) Any employee of the agency in his or her official capacity, or

(iii) Any employee of the agency in his or her official capacity where the Department of Justice has agreed to represent the employee, or

(iv) The United States, where the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the agency determines that their use of such records is relevant and necessary to the litigation, provided; however,

that in each case, the agency determines that disclosure of the records to the court or adjudicative body is a use of the information contained in the records that is compatible with the purpose for which it is collected.

(c) *Disclosure to third parties.* Personal information which may be disclosed under the Freedom of Information Act:

(1) On military personnel: Name, rank, date of rank, gross salary, present and past duty assignments, future assignments that are officially established, office or duty telephone number, source of commission, promotion sequence number, awards and decorations, military and civilian educational level, duty status at any given time.

(2) On civilian employees: Name, present and past position titles, grades, salaries, duty stations that include office or duty telephone numbers. However, disclosure of this information will not be made where the information requested is a list of present or past position titles, grades, salaries, and/or duty stations and, as such, is:

(i) Selected to constitute a clearly unwarranted invasion of personal privacy. For example, the nature of the request calls for a response that would reveal more about the employee than the five enumerated items;

(ii) Would be protected from mandatory disclosure under an exemption of the Freedom of Information Act.

(iii) In addition to the information in § 505.3(c)(2) above, the following information may be made available to a prospective employer of a current or former Army employee: Tenure of employment, civil service status, length of service in the Army and the Government and, date and reason for separation shown on the Notification of Personnel Action, SF 50.

(d) *Accounting of disclosure.* (1) An accounting of disclosure is required whenever a record from an Army system of records is disclosed to someone other than the data subject, except when that record:

(i) Is disclosed to officials within the Department of Defense who have a need for it in the performance of official business;

(ii) Is required to be disclosed under the Freedom of Information Act.

## Department of the Army, DoD

## § 505.4

(2) Since the characteristics of records maintained within the Army vary widely, no uniform method for keeping the disclosure of accounting is prescribed. For most paper records, the accounting may be affixed to the record being disclosed. It must be a written record and consist of:

(i) Description of the record disclosed;

(ii) Name, position title, and address of the person to whom disclosure was made;

(iii) Date, method, and purpose of the disclosure; and

(iv) Name and position title of the person making the disclosure.

(3) Purpose of the accounting of disclosure is to enable an individual:

(i) To ascertain those persons/agencies that have received information about the individual, and

(ii) To provide a basis for informing recipients of subsequent amendments or statements of dispute concerning the record.

(4) When an individual requests such an accounting, the system manager or designee shall respond within 10 work days and inform the individual of the items in § 505.3(d)(2) above.

(5) The only basis for not furnishing the data subject an accounting of disclosures are if disclosure was made for law enforcement purposes under 5 U.S.C. 552a(b)(7), or the disclosure was from a system of records for which an exemption from 5 U.S.C. 552a(c)(3) has been claimed (see appendix C to this part).

[50 FR 42164, Oct. 18, 1985, as amended at 58 FR 51013, Sept. 30, 1993]

### **§ 505.4 Record-keeping requirements under the Privacy Act.**

(a) *Systems of records.* (1) Notices of all Army systems of records are required by the Act to be published in the FEDERAL REGISTER. An example is at appendix A to this part. When new systems are established, or major changes occur in existing systems, which meet the criteria of OMB Guidelines summarized at § 505.4(f)(2), advance notice is required to be furnished OMB and the Congress before the system or proposed changes become operational.

(2) Uncirculated personal notes, papers and records which are retained at the author's discretion and over which the Army exercises no control or dominion are not considered Army records within the meaning of the Privacy Act. Individuals who maintain such notes must restrict their use of memory aids. Disclosure from personal notes, either intentional or through carelessness, remove the information from the category of memory aids and the notes then become subject to the provisions of the Act.

(3) Only personal information as is relevant and necessary to accomplish a purpose or mission of the Army, required by Federal statute or Executive Order of the President, will be maintained in Army systems of records. Statutory authority, or regulatory authority to establish and maintain a system of records does not convey unlimited authority to collect and maintain all information which may be useful or convenient. The authority is limited to relevant and necessary information.

(4) Except for statistical records, most records could be used to determine an individual's rights, benefits, or privileges. To ensure accuracy, personal information to be included in a system of records will be collected directly from the individual if possible. Collection of information from third parties should be limited to verifying information for security or employment suitability or obtaining performance data or opinion-type evaluations.

(b) *Privacy Act Statement.* Whenever personal information is requested from an individual that will become part of system of records retrieved by reference to the individual's names or other personal identifier, the individual will be furnished a Privacy Act Statement. This is to ensure that individuals know why the information is collected so they can make an informed decision on whether or not to furnish it. As a minimum, the Privacy Act Statement will include the following information in language that is explicit and easily understood and not so lengthy as to deter an individual from reading it:

(1) Cite the specific statute or Executive Order, including a brief title or

subject, that authorizes the Army to collect the personal information requested. Inform the individual whether or not a response is mandatory or voluntary, and any possible consequences of failing to respond.

(2) Cite the principal purpose(s) for which the information will be used; and

(3) Cite the probable routine uses for which the information may be used.

This may be a summary of information published in the applicable system notice. The above information normally should be printed on the form used to record the information. In certain instances, it may be printed in a public notice in a conspicuous location such as check-cashing facilities; however, if the individual requests a copy of its contents, it must be provided.

(c) *Social Security Number (SSN)*. Executive Order 9397 authorizes the Department of the Army to use the SSN as a system of identifying Army members and employees. Once a military member or civilian employee of the Department of the Army has disclosed his/her SSN for purposes of establishing personnel, financial, or medical records upon entry into Army service or employment, the SSN becomes his/her identification number. No other use of this number is authorized. Therefore, whether the SSN alone is requested from the individual, or the SSN together with other personal information, the Privacy Act Statement must make clear that disclosure of the number is voluntary. If the individual refuses to disclose his/her SSN, the Army activity must be prepared to identify the individual by alternate means.

(d) *Safeguarding personal information*. (1) The Privacy Act requires establishment of appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any threats or hazards to the subjects security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness.

(2) At each location, and for each system of records, an official will be designated to safeguard the information in that system. Consideration must be given to sensitivity of the data, need for accuracy and reliability in oper-

ations, general security of the area, cost of safeguards, etc. See AR 380-380.

(3) Ordinarily, personal information must be afforded at least the protection required for information designated "For Official Use Only" (see Chapter IV, AR 340-17). Privacy Act data will be afforded reasonable safeguards to prevent inadvertent or unauthorized disclosure of record content during processing, storage, transmission, and disposal.

(4) No comparisons of Army records systems with systems of other Federal or commercial agencies (known as "matching" or "computer matching" programs) will be accomplished without prior approval of the Assistant Chief of Staff for Information Management (DAIM-RMS-S), Alex, VA 22331-0301.

(e) First Amendment rights. No record describing how an individual exercises rights guaranteed by the First Amendment will be kept unless expressly authorized by Federal statute, by the individual about whom the record pertains, or unless pertinent to and within the scope of an authorized law enforcement activity. Exercise of these rights includes, but is not limited to, religious and political beliefs, freedom of speech and the press, and the right of assembly and to petition.

(f) *System notice*. (1) The Army publishes in the FEDERAL REGISTER a notice describing each system of records for which it is responsible. A notice contains:

(i) Name and location(s) of the records;

(ii) Categories of individuals on whom records are maintained;

(iii) Categories of records in the system;

(iv) Authority (statutory or Executive Order) authorizing the system;

(v) Purpose(s) of the system;

(vi) Routine uses of the records, including the categories of users and the purposes of such uses;

(vii) Policies and practices for storing, retrieving, accessing, retaining, and disposing of the records;

(viii) Position title and business address of the responsible official;

(ix) Procedures an individual must follow to learn if a system of records contains a record about the individual;

## Department of the Army, DoD

## § 505.5

(x) Procedures an individual must follow to gain access to a record about that individual in a system of records, to contest contents, and to appeal initial determinations;

(xi) Categories of sources of records in the system;

(xii) Exemptions from the Privacy Act claimed for the system. (See example notice at appendix A to this part.)

(2) New, or altered, systems which meet the requirements below, require a report to the Congress and the Office of Management and Budget. A new system is one for which no system notice is published in the FEDERAL REGISTER. An altered system is one that:

(i) Increases or changes the number or types of individuals on whom records are kept so that it significantly alters the character and purpose of the system of records.

(ii) Expands the types of categories of information maintained.

(iii) Alters the manner in which records are organized, indexed, or retrieved so as to change the nature or scope of those records.

(iv) Alters the purposes for which the information is used, or adds a routine use that is not compatible with the purpose for which the system is maintained.

(v) Changes the equipment configuration on which the system is operated so as to create potential for either greater or easier access.

(3) Report of a new or altered system must be sent to HQDA (DAIM-RMS-S) at least 120 days before the system or changes become operational, and include a narrative statement and supporting documentation.

(i) The narrative statement must contain the following items:

(A) System identification and name;

(B) Responsible official;

(C) Purpose(s) of the system, or nature of changes proposed (if an altered system);

(D) Authority for the system;

(E) Number (or estimate) of individuals on whom records will be kept;

(F) Information of First Amendment activities;

(G) Measure to assure information accuracy;

(H) Other measures to assure system security; (Automated systems require risk assessment under AR 380-380.)

(I) Relations to State/local government activities. (See example at appendix B to this part.)

(4) Supporting documentation consists of system notice for the proposed new or altered system, and proposed exemption rule, if applicable.

(g) *Reporting requirements.* (1) The annual report required by the Act, as amended by Pub. L. 97-375, 96 Stat. 1821, focuses on two primary areas:

(i) Information describing the exercise of individuals' rights of access to and amendment of records.

(ii) Changes in, or additions to, systems of records.

(2) Specific reporting requirements will be disseminated each year by The Assistant Chief of Staff for Information Management (DAIM-RMS-S) in a letter to reporting elements.

(h) *Rules of conduct.* System managers will ensure that all personnel, including government contractors or their employees, who are involved in the design, development, operation, maintenance, or control of any system of records, are informed of all requirements to protect the privacy of individuals who are subjects of the records.

(i) *Judicial sanctions.* The Privacy Act has both civil remedies and criminal penalties for violations of its provisions:

(1) Civil remedies: An individual may file a civil suit against the Army if Army personnel fail to comply with the Privacy Act.

(2) Criminal penalties: A member or employee of the Army may be guilty of a misdemeanor and fined not more than \$5,000 for willfully:

(i) Maintaining a system of records without first meeting the public notice requirements of publishing in the FEDERAL REGISTER;

(ii) Disclosing individually identifiable personal information to one not entitled to have it;

(iii) Asking for or getting another's record under false pretense.

### § 505.5 Exemptions.

(a) *Exempting systems of records.* The Secretary of the Army may exempt Army systems of records from certain

requirements of the Privacy Act. There are two kinds of exemptions: General and specific. The general exemption relieves systems of records from most requirements of the Act; the specific exemptions from only a few. See appendix C to this part.

(b) *General exemptions.* Only Army activities actually engaged in the enforcement of criminal laws as their primary function may claim the general exemption. To qualify for this exemption, a system must consist of:

(1) Information compiled to identify individual criminals and alleged criminals, which consists only of identifying data and arrest records; type and disposition of charges; sentencing, confinement, and release records; and parole and probation status;

(2) Information compiled for the purpose of criminal investigation including efforts to prevent, reduce, or control crime and reports of informants and investigators associated with an identifiable individual; or

(3) Reports identifiable to an individual, compile at any stage of the process of enforcement of the criminal laws, from arrest or indictment through release from supervision.

(c) *Specific exemptions.* The Secretary of the Army has exempted all properly classified information and a few systems of records that have the following kinds of information, from certain parts of the Privacy Act. The Privacy Act exemption cite appears in parentheses after each category.

(1) Classified information in every Army system of records. This exemption is not limited to the systems listed in Sec. 505.5(d). Before denying as individual access to classified information, the Access and Amendment Refusal Authority must make sure that it was properly classified under the standards of Executive Orders 11652, 12065, or 12958 and that it must remain so in the interest of national defense of foreign policy. (5 U.S.C. 552a(k)(1)).

(2) Investigatory data for law enforcement purposes (other than that claimed under the general exemption). However, if this information has been used to deny someone a right, privilege or benefit to which the individual is entitled by Federal law, it must be released, unless doing so would reveal the

identity of a confidential source. (5 U.S.C. 552a(k)(2)).

(3) Records maintained in connection with providing protective services to the President of the United States or other individuals protected pursuant to Title 18 U.S.C., section 3056. (5 U.S.C. 552a(k)(3)).

(4) Statistical data required by statute and used only for statistical purposes and not to make decisions on the rights, benefits, or entitlements of individuals, except for census records which may be disclosed under Title 13 U.S.C., section 8. (5 U.S.C. 552a(k)(4)).

(5) Data compiled to determine suitability, eligibility, or qualifications for Federal service, Federal contracts, or access to classified information. This information may be withheld only to the extent that disclosure would reveal the identity of a confidential source. (5 U.S.C. 552a(k)(5)).

(6) Testing material used to determine if a person is qualified for appointment or promotion in the Federal service. This information may be withheld only if disclosure would compromise the objectivity or fairness of the examination process. (5 U.S.C. 552a(k)(6)).

(7) Information to determine promotion potential in the Armed Forces. Information may be withheld, but only to the extent that disclosure would reveal the identity of a confidential source. (5 U.S.C. 552a(k)(7)).

(d) *Procedures.* When a system manager seeks an exemption for a system of records, the following information will be furnished to the Director of Information Systems for Command, Control, Communications and Computers, Washington, DC 20310-0107; applicable system notice, exemptions sought, and justification. After appropriate staffing and approval by the Secretary of the Army, a proposed rule will be published in the FEDERAL REGISTER, followed, by a final rule 60 days later. No exemption may be invoked until these steps have been completed.

(e) *Exempt Army records.* The following records may be exempt from certain parts of the Privacy Act:

(1) *System identifier:* A0020-1a SAIG

(i) *System name:* Inspector General Records.

## Department of the Army, DoD

## § 505.5

(ii) *Exemptions:* (A) Investigatory material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source.

(B) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(C) Therefore, portions of the system of records may be exempt pursuant to 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (e)(4)(I), and (f).

(iii) *Authority:* 5 U.S.C. 552a(k)(2) and (k)(5).

(iv) *Reason:* (A) From subsection (c)(3) because the release of the disclosure accounting, for disclosures pursuant to the routine uses published for this system, would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(B) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(C) From subsection (e)(1) because in the course of criminal investigations information is often obtained concerning the violations of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information is retained since it can aid in estab-

lishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(D) From subsections (e)(4)(G) and (e)(4)(H) because this system of records is exempt from individual access pursuant to subsection (k)(2) of the Privacy Act of 1974.

(E) From subsection (e)(4)(I) because of the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(F) From subsection (f) because this system of records has been exempted from the access provisions of subsection (d).

(G) Consistent with the legislative purpose of the Privacy Act of 1974, the Department of the Army will grant access to nonexempt material in the records being maintained. Disclosure will be governed by the Department of the Army's Privacy Regulation, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered, the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of this nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated in this paragraph. The decisions to release information from these systems will be made on a case-by-case basis.

(2) [Reserved]

(3) *A0025-55SAIS.*

(i) *System name:* Request for Information Files.

(ii) *Exemption:* (A) All portions of this system of records which fall within the scope of 5 U.S.C. 552a(j)(2) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5), (e)(8), (f) and (g).

(B) All portions of the system maintained by offices of Initial Denying Authorities which do not have a law enforcement mission and which fall within the scope of 5 U.S.C. 552a(k)(1) through (k)(7) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f).

(iii) *Authority*: 5 U.S.C. 552a(j)(2), and (k)(1) through (k)(7).

(iv) *Reasons*: This system of records is maintained solely for the purpose of administering the Freedom of Information Act and processing routine requests for information. To insure an accurate and complete file on each case, it is sometimes necessary to include copies of records which have been the subject of a Freedom of Information Act request. This situation applies principally to cases in which an individual has been denied access and/or amendment of personal records under an exemption authorized by 5 U.S.C. 552. The same justification for the original denial would apply to denial of access to copies maintained in the Freedom of Information Act file. It should be emphasized that the majority of records in this system are available on request to the individual and that all records are used solely to process requests. This file is not used to make any other determinations on the rights, benefits or privileges of individuals.

(4) *A0027-1DAJA*.

(i) *System name*: General Legal Files.

(ii) *Exemption*: All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(1), (k)(2), (k)(5), (k)(6), and (k)(7) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), and (f).

(iii) *Authority*: 5 U.S.C. 552a(k)(1), (k)(2), (k)(5), (k)(6), and (k)(7).

(iv) *Reasons*: Various records from other exempted systems of records are sometimes submitted for legal review or other action. A copy of such records may be permanently incorporated into the General Legal Files system of records as evidence of the facts upon which a legal opinion or review was based. Exemption of the General Legal Files system of records is necessary in order to ensure that such records continue to receive the same protection afforded them by exemptions granted

to the systems of records in which they were originally filed.

(5) *System identifier*: A0027-10a DAJA

(i) *System name*: Prosecutorial Files.

(ii) *Exemptions*: Parts of this system may be exempt pursuant to 5 U.S.C. 552a(j)(2) if the information is compiled and maintained by a component of the agency which performs as its principle function any activity pertaining to the enforcement of criminal laws. Therefore, portions of the system of records may be exempt pursuant to 5 U.S.C. 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (H) and (I), (e)(5), (e)(8), (f), and (g).

(iii) *Authority*: 5 U.S.C. 552a(j)(2).

(iv) *Reason*: (A) From subsection (c)(3) because the release of the disclosure accounting, for disclosures pursuant to the routine uses published for this system, would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(B) From subsection (c)(4) because an exemption is being claimed for subsection (d), this subsection will not be applicable.

(C) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(D) From subsection (e)(1) because in the course of criminal investigations information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(E) From subsection (e)(2) because in a criminal investigation the requirement that information be collected to the greatest extent possible from the

## Department of the Army, DoD

## § 505.5

subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection.

(F) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life and physical safety of confidential informants.

(G) From subsections (e)(4)(G) and (H) because this system of records is exempt from individual access pursuant to subsection (j)(2) of the Privacy Act of 1974.

(H) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(I) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment reporting on investigations and impede the development of intelligence necessary for effective law enforcement.

(J) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue search authorizations and could reveal investigative techniques and procedures.

(K) From subsection (f) because this system of records has been exempted from the access provisions of subsection (d).

(L) From subsection (g) because this system of records is compiled for law enforcement purposes and has been exempted from the access provisions of subsections (d) and (f).

(M) Consistent with the legislative purpose of the Privacy Act of 1974, the Department of the Army will grant access to nonexempt material in the records being maintained. Disclosure will be governed by the Department of the Army's Privacy Regulation (this part 505), but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered, the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of this nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated in this paragraph. The decisions to release information from these systems will be made on a case-by-case basis.

(6) *System identifier:* A0027-10b DAJA

(i) *System name:* Courts-Martial Records and Reviews.

(ii) *Exemptions:* Parts of this system may be exempt pursuant to 5 U.S.C. 552a(j)(2) if the information is compiled and maintained by a component of the agency which performs as its principle function any activity pertaining to the enforcement of criminal laws. Therefore, portions of this system of records may be exempt pursuant to 5 U.S.C. 552a(j)(2) from the following subsection of 5 U.S.C. 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (H) and (I), (e)(5), (e)(8), (f), and (g).

(iii) *Authority:* 5 U.S.C. 552a(j)(2).

(iv) *Reason:* (A) From subsection (c)(3) because the release of the disclosure accounting, for disclosures pursuant to the routine uses published for this system, would permit the subject



of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(B) From subsection (c)(4) because an exemption is being claimed for subsection (d), this subsection will not be applicable.

(C) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(D) From subsection (e)(1) because in the course of criminal investigations information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(E) From subsection (e)(2) because in a criminal investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection.

(F) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life and physical safety of confidential informants.

(G) From subsections (e)(4)(G) and (H) because this system of records is exempt from individual access pursuant to subsection (j)(2) of the Privacy Act of 1974.

(H) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(I) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of intelligence necessary for effective law enforcement.

(J) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue search authorizations and could reveal investigative techniques and procedures.

(K) From subsection (f) because this system of records has been exempted from the access provisions of subsection (d).

(L) From subsection (g) because this system of records is compiled for law enforcement purposes and has been exempted from the access provisions of subsections (d) and (f).

(M) Consistent with the legislative purpose of the Privacy Act of 1974, the Department of the Army will grant access to nonexempt material in the records being maintained. Disclosure will be governed by the Department of the Army's Privacy Regulation (this part 505), but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be

## Department of the Army, DoD

## § 505.5

endangered, the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of this nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated in this paragraph. The decisions to release information from these systems will be made on a case-by-case basis.

(7) *A0190-5DAMO.*

(i) *System name:* Vehicle Registration System (VRS).

(ii) *Exemption:* All portions of this system of records which fall within the scope of 5 U.S.C. 552a(j)(2) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (c)(4), (d), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(8), (f), and (g).

(iii) *Authority:* 5 U.S.C. 552a(j)(2).

(iv) *Reasons:* (A) From subsections (c)(4), (d), (e)(4)(G), (e)(4)(H), (f) and (g) because granting individuals access to information collected and maintained by this component relating to the enforcement of laws could interfere with proper investigations and the orderly administration of justice. Disclosure of this information could result in the concealment, alteration or destruction of evidence, the identification of offenders or alleged offenders, nature and disposition of charges; and jeopardize the safety and well-being of informants, witnesses and their families, and law enforcement personnel and their families. Disclosure of this information could also reveal and render ineffectual investigative techniques, sources and methods used by this component, and could result in the invasion of the privacy of individuals only incidentally related to an investigation. Exemption from access necessarily includes exemption from other requirements.

(B) From subsection (c)(3) because the release of accounting of disclosure would place the subject of an investigation on notice that he is under investigation and provide him with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(C) From subsection (e)(2) because in a criminal or other law enforcement

investigation, the requirement that information be collected to the greatest extent practicable from the subject individual would alert the subject as to the nature or existence of the investigation and thereby present a serious impediment to effective law enforcement.

(D) From subsection (e)(3) because compliance would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(E) From subsection (e)(8) because compliance with this provision would provide an impediment to law enforcement by interfering with the ability to issue warrants or subpoenas and by revealing investigative techniques, procedures or evidence.

(8) *A0190-9DAMO.*

(i) *System name:* Absentee Case Files.

(ii) *Exemption:* All portions of this system of records which fall within the scope of 5 U.S.C. 552a(j)(2) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (c)(4), (d), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(8), (f), and (g).

(iii) *Authority:* 5 U.S.C. 552a(j)(2).

(iv) *Reasons:* (A) From subsection (c)(4), (d), (e)(4)(G), (e)(4)(H), (f) and (g) because granting individuals access to information collected and maintained by this component relating to the enforcement of laws could interfere with proper investigations and the orderly administration of justice. Disclosure of this information could result in the concealment, alteration or destruction of evidence, the identification of offenders or alleged offenders, nature and disposition of charges; and jeopardize the safety and well-being of informants, witnesses and their families, and law enforcement personnel and their families. Disclosure of this information could also reveal and render ineffectual investigative techniques, sources and methods used by this component, and could result in the invasion of the privacy of individuals only incidentally related to an investigation. Exemption from access necessarily includes exemption from other requirements.

(B) From subsection (c)(3) because the release of accounting of disclosure

would place the subject of an investigation on notice that he is under investigation and provide him with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(C) From subsection (e)(2) because in a criminal or other law enforcement investigation, the requirement that information be collected to the greatest extent practicable from the subject individual would alert the subject as to the nature or existence of the investigation and thereby present a serious impediment to effective law enforcement.

(D) From subsection (e)(3) because compliance would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(E) From subsection (e)(8) because compliance with this provision would provide an impediment to law enforcement by interfering with the ability to issue warrants or subpoenas and by revealing investigative techniques, procedures or evidence.

(9) *A0190-14DAMO.*

(i) *System name:* Registration and Permit Files.

(ii) *Exemption:* All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(2) may be exempt from the provisions of 5 U.S.C. 552a(c)(3).

(iii) *Authority:* 5 U.S.C. 552a(k)(2).

(iv) *Reasons:* From subsection (c)(3) because the release of accounting of disclosures would place the subject of an investigation on notice that he or she is under investigation and provide him or her with significant information concerning the nature of the investigation thus resulting in a serious impediment to criminal law enforcement investigations, activities or the compromise of properly classified material.

(10) *A0190-30DAMO.*

(i) *System name:* Military Police Investigator Certification Files.

(ii) *Exemption:* All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(2), (k)(5), and (k)(7) may be exempt from the provisions

of 5 U.S.C. 552a(d), (e)(4)(G), (e)(4)(H), and (f).

(iii) *Authority:* 5 U.S.C. 552a(k)(2), (k)(5) and (k)(7).

(iv) *Reasons:* From subsections (d), (e)(4)(G), (e)(4)(H), and (f) because disclosure of portions of the information in this system of records would seriously impair selection and management of these uniquely functioning individuals; hamper the inclusion of comments, reports and evaluations concerning the performance, qualifications, character, actions, and propensities of the agency; and prematurely compromise investigations which either concern the conduct of the agent himself or herself, or investigations wherein he or she is integrally or only peripherally involved. Additionally, the exemption from access necessarily includes exemptions from the amendment and the agency procedures that would otherwise be required to process these types of requests.

(11) *A0190-40DAMO.*

(i) *System name:* Serious Incident Reporting Files.

(ii) *Exemption:* All portions of this system of records which fall within the scope of 5 U.S.C. 552a(j)(2) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (c)(4), (d), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(8), (f), and (g).

(iii) *Authority:* 5 U.S.C. 552a(j)(2).

(iv) *Reasons:* (A) From subsection (c)(4), (d), (e)(4)(G), (e)(4)(H), (f) and (g) because granting individuals access to information collected and maintained by this component relating to the enforcement of laws could interfere with proper investigations and the orderly administration of justice. Disclosure of this information could result in the concealment, alteration or destruction of evidence, the identification of offenders or alleged offenders, nature and disposition of charges, and jeopardize the safety and well-being of informants, witnesses and their families, and law enforcement personnel and their families. Disclosure of this information could also reveal and render ineffectual investigative techniques, sources, and methods used by this component, and could result in the invasion of the privacy of individuals only incidentally related to an investigation. Exemption

## Department of the Army, DoD

## § 505.5

from access necessarily includes exemption from the other requirements.

(B) From subsection (c)(3) because of the release of accounting of disclosure would place the subject of an investigation on notice that he is under investigation and provide him with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(C) From subsection (e)(2) because in a criminal or other law enforcement investigation, they require that information be collected to the greatest extent practicable from the subject individual would alert the subject as to the nature or existence of the investigation and thereby present a serious impediment to effective law enforcement.

(D) From subsection (e)(3) because compliance would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(E) From subsection (e)(8) because compliance with this provision would provide an impediment to law enforcement by interfering with the ability to issue warrants or subpoenas and be revealing investigative techniques, procedures or evidence.

(12) *System identifier:* A0190-45 DAMO

(i) *System name:* Offense Reporting System (ORS)

(ii) *Exemptions:* Parts of this system may be exempt pursuant to 5 U.S.C. 552a(j)(2) if the information is compiled and maintained by a component of the agency which performs as its principle function any activity pertaining to the enforcement of criminal laws. Therefore, portions of the system of records may be exempt pursuant to 5 U.S.C. 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (H) and (I), (e)(5), (e)(8), (f), and (g).

(iii) *Authority:* 5 U.S.C. 552a(j)(2).

(iv) *Reason:* (A) From subsection (c)(3) because the release of the disclosure accounting, for disclosures pursuant to the routine uses published for this system, would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a

serious impediment to law enforcement.

(B) From subsection (c)(4) because an exemption is being claimed for subsection (d), this subsection will not be applicable.

(C) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(D) From subsection (e)(1) because in the course of criminal investigations information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(E) From subsection (e)(2) because in a criminal investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection.

(F) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life and physical safety of confidential informants.

(G) From subsections (e)(4)(G) and (H) because this system of records is exempt from individual access pursuant to subsection (j)(2) of the Privacy Act of 1974.

(H) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal

and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(I) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment reporting on investigations and impede the development of intelligence necessary for effective law enforcement.

(J) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue search authorizations and could reveal investigative techniques and procedures.

(K) From subsection (f) because this system of records has been exempted from the access provisions of subsection (d).

(L) From subsection (g) because this system of records is compiled for law enforcement purposes and has been exempted from the access provisions of subsections (d) and (f).

(M) Consistent with the legislative purpose of the Privacy Act of 1974, the Department of the Army will grant access to nonexempt material in the records being maintained. Disclosure will be governed by the Department of the Army's Privacy Regulation, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered, the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible,

information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated above. The decisions to release information from these systems will be made on a case-by-case basis.

(13) *System identifier*: A0190-47 DAMO.

(i) *System name*: Correctional Reporting System (CRS).

(ii) *Exemption*. Parts of this system may be exempt pursuant to 5 U.S.C. 552a(j)(2) if the information is compiled and maintained by a component of the agency which performs as its principle function any activity pertaining to the enforcement of criminal laws. All portions of this system of records which fall within the scope of 5 U.S.C. 552a(j)(2) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (c)(4), (d), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g).

Consistent with the legislative purpose of the Privacy Act of 1974, the Department of the Army will grant access to nonexempt material in the records being maintained. Disclosure will be governed by the Department of the Army's Privacy Regulation, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered, the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated above. The decisions to release information from these systems will be made on a case-by-case basis necessary for effective law enforcement.

(iii) *Authority*: 5 U.S.C. 552a(j)(2).

(iv) *Reasons*: (A) From subsection (c)(3) because the release of the disclosure accounting, or disclosures pursuant to the routine uses published for

## Department of the Army, DoD

## § 505.5

this system, would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(B) From subsection (c)(4) because an exemption is being claimed for subsection (d), this subsection will not be applicable.

(C) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(D) From subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life and physical safety of confidential informants.

(E) From subsections (e)(4)(G) and (H) because this system of records is exempt from individual access pursuant to subsections (j)(2) of the Privacy Act of 1974.

(F) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(G) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e) (5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment reporting on investigations and impede the development of intelligence

necessary for effective law enforcement.

(H) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue search authorizations and could reveal investigative techniques and procedures.

(I) From subsection (f) because this system of records has been exempted from the access provisions of subsection (d).

(J) From subsection (g) because this system of records compiled for lawenforcement purposes and has been exempted from the access provisions of subsections (d) and (f).

(14) *A0195-2aUSACIDC.*

(i) *System name:* Source Register.

(ii) *Exemption:* All portions of this system of records which fall within the scope of 5 U.S.C. 552a(j)(2) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(5), (e)(8), (f), and (g).

(iii) *Authority:* 5 U.S.C. 552a(j)(2).

(iv) *Reasons:* (A) From subsection (c)(3) because release of accounting of disclosures would provide the informant with significant information concerning the nature of a particular investigation, the internal methods and techniques involved in criminal investigation, and the investigative agencies (state, local or foreign) involved in a particular case resulting in a serious compromise of the criminal law enforcement processes.

(B) From subsection (c)(4), (d), (e)(4)(G), (e)(4)(H), (f), and (g) because disclosure of portions of the information in this system of records would seriously impair the prudent and efficient handling of these uniquely functioning individuals; hamper the inclusion of comments and evaluations concerning the performance qualification, character, identity, and propensities of the informant; and prematurely compromise criminal investigations which either concern the conduct of the informant himself or investigations wherein he/she is integrally or only peripherally involved. Additionally, the exemption from access necessarily includes exemption from amendment, certain agency requirements relating

to access and amendment of records and civil liability predicated upon agency compliance with specific provisions of the Privacy Act.

(C) From subsection (d), (e)(4)(G), (e)(4)(H), and (f) are also necessary to protect the security of information properly classified in the interest of national defense and foreign policy.

(D) From subsection (e)(1) because the nature of the criminal investigative function creates unique problems in prescribing what information concerning informants is relevant or necessary. Due to close liaison and existing relationships with other Federal, state, local and foreign law enforcement agencies, information about informants may be received which may relate to a case then under the investigative jurisdiction of another Government agency but it is necessary to maintain this information in order to provide leads for appropriate law enforcement purposes and to establish patterns of activity which may relate to the jurisdiction of both the USACIDC and other agencies. Additionally, the failure to maintain all known information about informants could affect the effective utilization of the individual and substantially increase the operational hazards incumbent in the employment of an informant in very compromising and sensitive situations.

(E) From subsection (e)(2) because collecting information from the informant would potentially thwart both the criminal investigative process and the required management control over these individuals by appraising the informant of investigations or management actions concerning his involvement in criminal activity or with USACIDC personnel.

(F) From subsection (e)(3) because supplying an informant with a form containing the information specified could result in the compromise of an investigation, tend to inhibit the cooperation of the informant, and render ineffectual investigative techniques and methods utilized by USACIDC in the performance of its criminal law enforcement duties.

(G) From subsection (e)(5) because this requirement would unduly hamper the criminal investigative process due

to type of records maintained an necessity for rapid information retrieval and dissemination. Also, in the collection of information about informants, it is impossible to determine what information is then accurate, relevant, timely and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation or contact brings new details to light. In the criminal investigative process, accuracy and relevance of information concerning informants can only be determined in a court of law. The restrictions imposed by subsection (e)(5) would restrict the ability of trained investigators to exercise their judgment in reporting information relating to informant's actions and would impede the development of criminal intelligence necessary for effective law enforcement.

(H) From subsection (e)(8) because the notice requirements of this provision could present a serious impediment to criminal law enforcement by revealing investigative techniques, procedures, and the existence of confidential investigations.

(15) *A0195-2bUSACIDC.*

(i) *System name:* Criminal Investigation and Crime Laboratory Files.

(ii) *Exemption:* All portions of this system of records which fall within the scope of 5 U.S.C. 552a(j)(2) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5), (e)(8), (f), and (g).

(iii) *Authority:* 5 U.S.C. 552(j)(2).

(iv) *Reasons:* (A) From subsection (c)(3) because the release of accounting of disclosures would place the subject of an investigation on notice that he is under investigation and provide him with significant information concerning coordinated investigative effort and techniques and the nature of the investigation, resulting in a serious impediment to criminal law enforcement activities or the compromise of properly classified material.

(B) From subsections (c)(4), (d), (e)(4)(G), (e)(4)(H), (f), and (g) because access might compromise on-going investigations, reveal classified information, investigatory techniques or the identity of confidential informants, or

## Department of the Army, DoD

## § 505.5

invade the privacy of persons who provide information in connection with a particular investigation. The exemption from access necessarily includes exemption from amendment, certain agency requirements relating to access and amendment of records, and civil liability predicated upon agency compliance with those specific provisions of the Privacy Act. The exemption from access necessarily includes exemption from other requirements.

(C) From subsection (e)(1) because the nature of the investigative function creates unique problems in prescribed specific perimeters in a particular case as to what information is relevant or necessary. Also, due to close liaisons and working relationships with other Federal, state, local, and foreign law enforcement agencies, information may be received which may relate to a case then under the investigative jurisdiction of another Government agency but it is necessary to maintain this information in order to provide leads for appropriate law enforcement purposes and to establish patterns of activity which may relate to the jurisdiction of both the USACIDC and other agencies.

(D) From subsection (e)(2) because collecting information from the subject of criminal investigations would thwart the investigative process by placing the subject of the investigation on notice thereof.

(E) From subsection (e)(3) because supplying an individual with a form containing the information specified could result in the compromise of an investigation, tend to inhibit the co-operation of the individual queried, and render ineffectual investigation techniques and methods utilized by USACIDC in the performance of their criminal law enforcement duties.

(F) From subsection (e)(5) because this requirement would unduly hamper the criminal investigative process due to the great volume of records maintained and the necessity for rapid information retrieval and dissemination. Also, in the collection of information for law enforcement purposes, it is impossible to determine what information is then accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance

as further investigation brings new details to light. In the criminal investigation process, accuracy and relevance of information can only be determine in a court of law. The restrictions imposed by subsection (e)(5) would restrict the ability of trained investigators to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement.

(G) From subsection (e)(8) because the notice requirements of this provision could present a serious impediment to criminal law enforcement by revealing investigative techniques, procedures, and the existence of confidential investigations.

(16) *A0195-6USACIDC.*

(i) *System name:* Criminal Investigation Accreditation and Polygraph Examiner Evaluation Files.

(ii) *Exemption:* All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(2), (k)(5), or (k)(7) may be exempt from the provisions of 5 U.S.C. 552a(d), (e)(1), (e)(4)(G), (e)(4)(H), and (f).

(iii) *Authority:* 5 U.S.C. 552a(k)(2), (k)(5), and (k)(7).

(iv) *Reasons:* (A) From subsections (d), (e)(4)(G), (e)(4)(H), and (f) because disclosure of portions of the information in this system of records would seriously impair the selection and management of these uniquely functioning individuals; hamper the inclusion of comments, reports and evaluations concerning the performance, qualifications, character, action and propensities of the agent; and prematurely compromise investigations with either concern the conduct of the agent himself or investigations wherein he or she is integrally or only peripherally involved. Additionally, the exemption from access necessarily includes exemptions from the amendment and the agency procedures which would otherwise be required to process these types of requests.

(B) From subsection (e)(1) because the failure to maintain all known information about agents could affect the effective utilization of the individual and substantially increase the operational hazards incumbent in the



employment of agents in very compromising and sensitive situations.

(17) *A0210-7DAMO*.

(i) *System name*: Expelled or Barred Person Files.

(ii) *Exemption*: All portions of this system of records which fall within the scope of 5 U.S.C. 552a(j)(2) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (c)(4), (d), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(8), (f), and (g).

(iii) *Authority*: 5 U.S.C. 552a(j)(2).

(iv) *Reasons*: (A) From subsection (c)(4), (d), (e)(4)(G), (e)(4)(H), (f) and (g) because granting individuals access to information collected and maintained by this component relating to the enforcement of laws could interfere with proper investigations and the orderly administration of justice. Disclosure of this information could result in the concealment, alteration or destruction of evidence, the identification of offenders or alleged offenders, nature and disposition of charges, and jeopardize the safety and well-being of informants, witnesses and their families, and law enforcement personnel and their families. Disclosure of this information could also reveal and render ineffectual investigative techniques, sources, and methods used by this component, and could result in the invasion of the privacy of individuals only incidentally related to an investigation. Exemption from access necessarily includes exemption from the other requirements.

(B) From subsection (c)(3) because of the release of accounting of disclosure would place the subject of an investigation on notice that he is under investigation and provide him with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(C) From subsection (e)(2) because in a criminal or other law enforcement investigation, they require that information be collected to the greatest extent practicable from the subject individual would alert the subject as to the nature or existence of the investigation and thereby present a serious impediment to effective law enforcement.

(D) From subsection (e)(3) because compliance would constitute a serious impediment to law enforcement in that it could compromise the existence of a

confidential investigation or reveal the identity of witnesses or confidential informants.

(E) From subsection (e)(8) because compliance with this provision would provide an impediment to law enforcement by interfering with the ability to issue warrants or subpoenas and be revealing investigative techniques, procedures or evidence.

(18) *System identifier*: A0025 JDIM

(i) *System name*: HQDA Correspondence and Control/Central Files System.

(ii) *Exemptions*: Documents within this system of records are generated by other elements of the Department of the Army or are received from other agencies and individuals. Because of the broad scope of the contents of this system of records, and since the introduction of documents is largely unregulatable, specific portions or documents that may require an exemption can not be predetermined. Therefore, and to the extent that such material is received and maintained, selected individual documents may be exempt.

(A) Information specifically authorized to be classified under E.O. 12958, as implemented by DoD 5200.1-R, may be exempt pursuant to 5 U.S.C. 552a(k)(1).

(B) Investigatory material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source.

(C) Records maintained in connection with providing protective services to the President and other individuals under 18 U.S.C. 3506, may be exempt pursuant to 5 U.S.C. 552a(k)(3).

(D) Records maintained solely for statistical research or program evaluation purposes and which are not used to make decisions on the rights, benefits, or entitlement of an individual except for census records which may be disclosed under 13 U.S.C. 8, may be exempt pursuant to 5 U.S.C. 552a(k)(4).

(E) Investigatory material compiled solely for the purpose of determining

## Department of the Army, DoD

## § 505.5

suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(F) Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service may be exempt pursuant to 5 U.S.C. 552a(k)(6), if the disclosure would compromise the objectivity or fairness of the test or examination process.

(G) Evaluation material used to determine potential for promotion in the Military Services may be exempt pursuant to 5 U.S.C. 552a(k)(7), but only to the extent that the disclosure of such material would reveal the identity of a confidential source.

(H) Portions of this system of records may be exempt pursuant to 5 U.S.C. 552a (k)(1) through (k)(7) from subsections (c)(3), (d), (e)(1), (e)(4)(G) and (H), and (f).

(iii) *Authority:* 5 U.S.C. 552a(k)(1) through (k)(7).

(iv) *Reasons:* (A) From subsection (c)(3) because the release of the disclosure accounting could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation and the fact that they are subjects of the investigation. It could permit the subject of an investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(B) From subsection (d) because access to the records contained in this system would inform the subject of an investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection of apprehension, and would present a serious impediment to law enforcement.

(C) From subsection (e)(1) because in the course of criminal investigations information is often obtained concerning the violation of laws or civil obligations of others not relating to ac-

tive case or matter. In the interest of effective law enforcement, it is necessary that this information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(D) From subsections (e)(4)(G) and (H) because this system of records is exempt from individual access pursuant to subsections (k)(2) of the Privacy Act of 1974.

(E) From subsection (f) because this system of records has been exempted from the access provisions of subsection (d).

(19) *System identifier:* A0340-21 TAPC

(i) *System name:* Privacy Case Files.

(ii) *Exemption:* During the processing of a Privacy Act request (which may include access requests, amendment requests, and requests for review for initial denials of such requests), exempt materials from other systems of records may in turn become part of the case record in this system. To the extent that copies of exempt records from those 'other' systems of records are entered into this system, the Department of the Army hereby claims the same exemptions for the records from those 'other' systems that are entered into this system, as claimed for the original primary system of which they are a part.

(iii) *Authority:* 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), (k)(3), (k)(4), (k)(5), (k)(6), and (k)(7).

(iv) Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent such provisions have been identified and an exemption claimed for the original record and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. In general, the exemptions were claimed in order to protect properly classified information relating to national defense and foreign policy, to avoid interference during the conduct of criminal, civil, or administrative actions or investigations, to ensure protective services provided the President and others are not compromised, to protect the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations, and

to preserve the confidentiality and integrity of Federal evaluation materials. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

(20) [Reserved]

(21) *A0351-12DAPE*.

(i) *System name*: Applicants/Students, U.S. Military Academy Prep School.

(ii) *Exemption*: All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(5) and (k)(7) may be exempt from the following provision of 5 U.S.C. 552a(d).

(iii) *Authority*: 5 U.S.C. 552a(k)(5) and (k)(7).

(iv) *Reasons*: It is imperative that the confidential nature of evaluation material on individuals, furnished to the US Military Academy Preparatory School under an express promise of confidentiality, be maintained to ensure the candid presentation of information necessary in determinations involving admission to or retention at the United States Military Academy and suitability for commissioned military service.

(22) *A0351-17aUSMA*.

(i) *System name*: U.S. Military Academy Candidate Files.

(ii) *Exemption*: All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(5), (k)(6), or (k)(7) may be exempt from the provisions of 5 U.S.C. 552a(d).

(iii) *Authority*: 5 U.S.C. 552a(k)(5), (k)(6) and (k)(7).

(iv) *Reasons*: (A) From subsection (d) because access might reveal investigatory and testing techniques. The exemption from access necessarily includes exemption from amendment, certain agency requirements relating to access and amendment of records, and civil liability predicated upon agency compliance with those specific provisions of the Privacy Act.

(B) Exemption is necessary to protect the identity of individuals who furnished information to the United States Military Academy which is used in determining suitability, eligibility, or qualifications for military service and which was provided under an express promise of confidentiality.

(C) Exemption is needed for the portion of records compiled within the Academy which pertain to testing or examination material used to rate individual qualifications, the disclosure of which would compromise the objectivity or fairness of the testing or examination process.

(D) Exemption is required for evaluation material used by the Academy in determining potential for promotion in the Armed Services, to protect the identity of a source who furnished information to the Academy under an express promise of confidentiality.

(23) *A0351-17bUSMA*.

(i) *System name*: U.S. Military Academy Personnel Cadet Records.

(ii) *Exemption*: All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(5) or (k)(7) may be exempt from the provisions of 5 U.S.C. 552a(d).

(iii) *Authority*: 5 U.S.C. 552a(k)(5) and (k)(7).

(iv) *Reasons*: It is imperative that the confidential nature of evaluation and investigatory material on candidates, cadets, and graduates, furnished to the United States Military Academy under promise of confidentiality be maintained to insure the candid presentation of information necessary in determinations involving admissions to the Military Academy and suitability for commissioned service and future promotion.

(24) *A0380-13DAMO*.

(i) *System name*: Local Criminal Intelligence Files.

(ii) *Exemption*: All portions of this system of records which fall within the scope of 5 U.S.C. 552a(j)(2) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (c)(4), (d), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(8), (f), and (g).

(iii) *Authority*: 5 U.S.C. 552a(j)(2).

(iv) *Reasons*: (A) From subsections (e)(4)(G), (e)(4)(H), (f), and (g) because granting individuals access to information collected and maintained by this component relating to the enforcement of laws could interfere with proper investigations and the orderly administration of justice. Disclosure of this information could result in the concealment, alteration or destruction of evidence, the identification of offenders or

alleged offenders, nature and disposition of charges; and jeopardize the safety and well-being of informants, witnesses and their families, and law enforcement personnel and their families. Disclosure of this information could also reveal and render ineffectual investigative techniques, sources and methods used by this component and could result in the invasion of the privacy of individuals only incidentally related to an investigation. Exemption from access necessarily includes exemption from the other requirements.

(B) From subsection (c)(3) because the release of accounting of disclosure would place the subject of an investigation on notice that he is under investigation and provide him with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement investigations.

(C) From subsection (e)(2) because, in a criminal or other law enforcement investigation, the requirement that information be collected to the greatest extent practicable from the subject individual would alert the subject as to the nature or existence of the investigation and thereby present a serious impediment to effective law enforcement.

(D) From subsection (e)(3) because compliance would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(E) From subsection (e)(8) because compliance with this provision would provide an impediment to law enforcement by interfering with the ability to issue warrants or subpoenas and by revealing investigative techniques, procedures or evidence.

(25) *A0380-67DAMI.*

(i) *System name:* Personnel Security Clearance Information Files.

(ii) *Exemption:* All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(1), (k)(2), or (k)(5) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (e)(4)(I).

(iii) *Authority:* 5 U.S.C. 552a(k)(1), (k)(2), or (k)(5).

(iv) *Reasons:* The material contained in this record system contains data concerning sensitive sources and operational methods whose dissemination must be strictly controlled because of national security intelligence considerations. Disclosure of documents or the disclosure accounting record may compromise the effectiveness of the operation, and negate specialized techniques used to support intelligence or criminal investigative programs, or otherwise interfere with the orderly conduct of intelligence operations or criminal investigations.

(26) *A0381-20bDAMI.*

(i) *System name:* Counterintelligence/Security Files.

(ii) *Exemption:* All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(1), (k)(2), and (k)(5) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d)(1) through (d)(5), (e)(1), (e)(4)(G), (e)(4)(H), and (e)(4)(I), and (f).

(iii) *Authority:* 5 U.S.C. 552a(k)(1), (k)(2), and (k)(5).

(iv) *Reasons:* (A) From subsection (c)(3) because disclosing the agencies to which information from this system has been released could inform the subject of an investigation of an actual or potential criminal violation, or intelligence operation or investigation; or the existence of that investigation or operation; of the nature and scope of the information and evidence obtained as to his/her activities or of the identity of confidential sources, witnesses, and intelligence personnel and could provide information to enable the subject to avoid detection or apprehension. Granting access to such information could seriously impede or compromise an investigation; endanger the physical safety of confidential sources, witnesses, intelligence personnel, and their families; lead to the improper influencing of witnesses; the destruction of evidence or the fabrication of testimony and disclose investigative techniques and procedures. In addition, granting access to such information could disclose classified and sensitive sources, information, and operational methods and could constitute an unwarranted invasion of the personal privacy of others.

(B) From subsection (d)(1) through (d)(5) because granting access to records in this system of records could inform the subject of a counterintelligence operation or investigation of an actual or potential criminal violation or the existence of that operation or investigation; of the nature and scope of the information and evidence obtained as to his/her activities; or of the identity of confidential sources, witnesses and intelligence personnel and could provide information to enable the subject to avoid detection or apprehension. Granting access to such information could seriously impede or compromise an operation or investigation; endanger the physical safety of confidential sources, witnesses, intelligence personnel and their families; lead to the improper influencing of witnesses; the destruction of evidence or the fabrication of testimony and disclose investigative techniques and procedures. In addition, the agency is required to protect the confidentiality of sources who furnished information to the Government under an expressed promise of confidentiality or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. This confidentiality is needed to maintain the Government's continued access to information from persons who otherwise might refuse to give it.

(C) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of specific information in the early stages of an investigation or operation. Relevance and necessity are often questions of judgement and timing, and it is only after the information is evaluated that the relevance and necessity of such information can be established. In addition, during the course of the investigation or operation, the investigator may obtain information which is incidental to the main purpose of the investigative jurisdiction of another agency. Such information cannot readily be segregated. Furthermore, during the course of the investigation or operation, the investigator may obtain information concerning violations of laws other than those which are within the scope of his/her jurisdiction. In the interest of effective intelligence oper-

ations and law enforcement, military intelligence agents should retain information, since it is an aid in establishing patterns of criminal or intelligence activity and provide valuable leads for other law enforcement or intelligence agencies.

(D) From subsection (e)(4)(G), (e)(4)(H), and (f) because this system or records is being exempt from subsections (d) of the Act, concerning access to records. These requirements are inapplicable to the extent that this system of records will be exempt from subsections (d)(1) through (d)(5) of the Act. Although the system would be exempt from these requirements, the Deputy Chief of Staff for Intelligence has published information concerning its notification, access, and contest procedures because under certain circumstances, the Deputy Chief of Staff for Intelligence could decide it is appropriate for an individual to have access to all or a portion of his/her records in this system of records.

(E) From subsection (e)(4)(I) because it is necessary to protect the confidentiality of the sources of information, to protect the privacy and physical safety of confidential sources and witnesses and to avoid the disclosure of investigative techniques and procedures. Although the system will be exempt from this requirement, the Deputy Chief of Staff for Intelligence has published such a notice in broad, generic terms.

(27) *A0381-100aDAMI*.

(i) *System name*: Intelligence/Counterintelligence Source Files.

(ii) *Exemption*: All portions of this system of records that fall within the scope of 5 U.S.C. 552a(k)(1), (k)(2), or (k)(5) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d)(1) through (d)(5), (e)(1), (e)(4)(G), (e)(4)(H), and (e)(4)(I), and (f).

(iii) *Authority*: 5 U.S.C. 552a(k)(1), (k)(2), and (k)(5).

(iv) *Reasons*: (A) From subsection (c)(3) because disclosing the agencies to which information from this system has been released could reveal the subject's involvement in a sensitive intelligence or counterintelligence operation or investigation of an actual or potential criminal violation, or intelligence operation or investigation; or the existence of that investigation or

operation. Granting access to such information could seriously impede or compromise an investigation or operation; endanger the physical safety of participants and their families, confidential sources, witnesses, intelligence personnel, and their families; and lead to the improper influencing of witnesses; the destruction of evidence or the fabrication of testimony and disclose investigative techniques and procedures.

(B) From subsection (d)(1) through (d)(5) because granting access to records could inform the subject of an intelligence or counterintelligence operation or investigation of an actual or potential criminal violation or the existence of that operation or investigation; or the nature and scope of the information and evidence obtained, or of the identity of confidential sources, witnesses and intelligence personnel. Granting access to such information could seriously impede or compromise an operation or investigation; endanger the physical safety of confidential sources, witnesses, intelligence personnel and their families; lead to the improper influencing of witnesses; the destruction of evidence or the fabrication of testimony; disclose investigative techniques and procedures; invade the privacy of those individuals involved in intelligence programs and their families; compromise and thus negate specialized techniques used to support intelligence programs; and interfere with and negate the orderly conduct of intelligence and counterintelligence operations and investigations. In addition, the agency is required to protect the confidentiality of sources who furnished information to the Government under an expressed promise of confidentiality or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. This confidentiality is needed to maintain the Government's continued access to information from persons who otherwise might refuse to give it.

(C) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of specific information in the early stages of an investigation or operation. Relevance and necessity are often questions of judgment

and timing, and it is only after the information is evaluated that the relevance and necessity of such information can be established. In addition, during the course of the investigation or operation, the investigator or operative may obtain information which is incidental to the main purpose of the investigative jurisdiction of another agency. Such information cannot readily be segregated. Furthermore, during the course of the investigation or operation, the investigator may obtain information concerning violations of law other than those which are within the scope of his/her jurisdiction. In the interest of effective intelligence operations and law enforcement, military intelligence agents should retain information, since it is an aid in establishing patterns of criminal or intelligence activity and provides valuable leads for other law enforcement or intelligence agencies.

(D) From subsection (e)(4)(G), (e)(4)(H), and (f) because this system of records is being exempt from subsection (d) of the Act concerning access to records. These requirements are inapplicable to the extent that this system of records will be exempt from subsections (d)(1) through (d)(5) of the Act. Although the system would be exempt from these requirements, the Deputy Chief of Staff for Intelligence has published information concerning its notification, access, and contest procedures because under certain circumstances, the Deputy Chief of staff for Intelligence could decide it is appropriate for an individual to have access to all or a portion of his/her records in this system of records.

(E) From subsection (e)(4)(I) because it is necessary to protect the confidentiality of sources of information, to protect the privacy and physical safety of participants and their families, confidential sources, and witnesses and to avoid the disclosure of specialized techniques and procedures. Although the system will be exempt from this requirement, the Deputy Chief of Staff for Intelligence has published such a notice in broad generic terms.

(28) *A0381-100bDAMI*

(i) *System name:* Technical Surveillance Index.

(ii) *Exemption:* All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(1), (k)(2), and (k)(5) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d)(1) through (d)(5), (e)(1), (e)(4)(G), (e)(4)(H), and (e)(4)(I).

(iii) *Authority:* 5 U.S.C. 552a(k)(1), (k)(2) or (k)(5).

(iv) *Reasons:* (A) From subsection (c)(3) because disclosing the identities of agencies to which information from this system has been released could inform the subject of an investigation of an actual or potential criminal violation or intelligence operation; of the existence of that investigation or operation; of the nature and scope of the information and evidence obtained as to his/her activities or of the identify of confidential sources, witnesses, and intelligence or law enforcement personnel and could provide information to enable the subject to avoid detection or apprehension. Granting access to such information could seriously impede or compromise an investigation; endanger the physical safety of confidential sources, witnesses, intelligence or law enforcement personnel, and their families; lead to the improper influencing of witnesses; the destruction of evidence or the fabrication of testimony and disclose investigative techniques and procedures. In addition, granting access to such information could disclose classified and sensitive sources and operational methods and could constitute an unwarranted invasion of the personal privacy of others.

(B) From subsection (d)(1) through (d)(5) because granting access to records in this system of records could inform the subject of an investigation of an actual or potential criminal violation; of the existence of that investigation; of the nature and scope of the information and evidence obtained as to his/her activities; or of the identity of confidential sources, witnesses and intelligence or law enforcement personnel and could provide information to enable the subject to avoid detection or apprehension. Granting access to such information could seriously impede or compromise an investigation; endanger the physical safety of confidential sources, witnesses, intelligence or law enforcement personnel

and their families; lead to the improper influencing of witnesses; the destruction of evidence or the fabrication of testimony and disclose investigative techniques and procedures. In addition, granting access to such information could disclose classified, sensitive sources and operational methods and could constitute an unwarranted invasion of the personal privacy of others.

(C) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of specific information in the early stages of an investigation or operation. Relevance and necessity are often questions of judgment and timing, and it is only after the information is evaluated that the relevance and necessity of such information can be established. In addition, during the course of the investigation or operation, the investigator may obtain information which is incidental to the main purpose of the investigative jurisdiction of another agency. Such information cannot readily be segregated. Furthermore, during the course of the investigation or operation, the investigator may obtain information concerning violation of laws other than those which are within the scope of his/her jurisdiction. In the interest of effective intelligence operations and law enforcement, criminal law enforcement investigators and military intelligence agents should retain this information, since it can aid in establishing patterns of criminal or intelligence activity and can provide valuable leads for other law enforcement or intelligence agencies.

(D) From subsections (e)(4)(G) and (e)(4)(H) because this system of records is being exempt from subsections (d) of the Act, concerning access to records, these requirements are inapplicable to the extent that this system of records will be exempt from subsections (d)(1) through (d)(5) of the Act. Although the system would be exempt from these requirements, the Deputy Chief of Staff for Intelligence and the U.S. Army Criminal Investigations Command have published information concerning its notification, access, and contest procedures for their respective areas because, under certain circumstances,

## Department of the Army, DoD

## § 505.5

the Deputy Chief of Staff for Intelligence or the U.S. Army Criminal Investigations Command could decide it is appropriate for an individual to have access to all or a portion of his/her records in this system of records.

(E) From subsection (e)(4)(I) because it is necessary to protect the confidentiality of the sources of information, to protect the privacy and physical safety of confidential sources and witnesses and to avoid the disclosure of investigative techniques and procedures. Although the system will be exempt from this requirement, the Deputy Chief of Staff for Intelligence and the U.S. Army Criminal Investigations Command have published such a notice in broad, generic terms.

(29) *System identifier:* A0601-141 DASG.

(i) *System name:* Applications for Appointment to Army Medical Department.

(ii) *Exemption:* Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source. Therefore, portions of the system of records may be exempt pursuant to 5 U.S.C. 552a(d).

(iii) *Authority:* 5 U.S.C. 552a(k)(5).

(iv) *Reasons:* It is imperative that the confidential nature of evaluations and investigatory material on applicants applying for enlistment furnished to the US Army Recruiting Command under an express promise of confidentiality, be maintained to insure the candid presentation of information necessary in determinations of enlistment and suitability for enlistment into the United States Army.

(30) *A0601-210aUSAREC.*

(i) *System name:* Enlisted Eligibility Files.

(ii) *Exemption:* All portions of this system of records which fall within the scope of 5 U.S.C. 552a(k)(5) may be exempt from the provisions of 5 U.S.C. 552a(d).

(iii) *Authority:* 5 U.S.C. 552a(k)(5).

(iv) *Reasons:* It is imperative that the confidential nature of evaluations and

investigatory material on applicants applying for enlistment furnished to the US Army Recruiting Command under an express promise of confidentiality, be maintained to insure the candid presentation of information necessary in determinations of enlistment and suitability for enlistment into the United States Army.

(31) *System identifier:* A0601-222 USMEPCOM

(i) *System name:* Armed Services Military Accession Testing

(ii) *Exemption:* Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service or military service may be exempt pursuant to 5 U.S.C. 552a(k)(6), if the disclosure would compromise the objectivity or fairness of the test or examination process. Therefore, portions of the system of records may be exempt pursuant to 5 U.S.C. 552a(d).

(iii) *Authority:* 5 U.S.C. 552a(k)(6).

(iv) *Reasons:* An exemption is required for those portions of the Skill Qualification Test system pertaining to individual item responses and scoring keys to preclude compromise of the test and to insure fairness and objectivity of the evaluation system.

(32) *System identifier:* A0608-18 DASG.

(i) *System name:* Army Family Advocacy Program (FAP) Files

(ii) *Exemptions:* (A) Investigatory material compiled for law enforcement purposes may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source.

(B) Investigative material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.



(C) Therefore, portions of the system of records may be exempt pursuant to 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f).

(iii) *Authority*: 5 U.S.C. 552a(k)(2) and (k)(5).

(iv) *Reason*: (A) From subsection (c)(3) because the release of the disclosure accounting, for disclosures pursuant to the routine uses published for this system, would permit the subject of a criminal investigation or matter under investigation to obtain valuable information concerning the nature of that investigation which will present a serious impediment to law enforcement.

(B) From subsection (d) because access to the records contained in this system would inform the subject of a criminal investigation of the existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and would present a serious impediment to law enforcement.

(C) From subsection (e)(1) because in the course of criminal investigations, information is often obtained concerning the violation of laws or civil obligations of others not relating to an active case or matter. In the interests of effective law enforcement, it is necessary that this valuable information be retained since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought.

(D) From subsections (e)(4)(G) and (H) because this system of records is exempt from individual access pursuant to subsections (k)(2) and (k)(5) of the Privacy Act of 1974.

(E) From subsection (e)(4)(I) because the identity of specific sources must be withheld in order to protect the confidentiality of the sources of criminal and other law enforcement information. This exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(F) From subsection (f) because this system of records has been exempted from the access provisions of subsection (d).

(G) Consistent with the legislative purpose of the Privacy Act of 1974, the Department of the Army will grant ac-

cess to nonexempt material in the records being maintained. Disclosure will be governed by the Department of the Army's Privacy Regulation, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered, the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated above. The decisions to release information from these systems will be made on a case-by-case basis.

(33) *A0614-115DAMI*.

(i) *System name*: Department of the Army Operational Support Activities.

(ii) *Exemption*: All portions of this system of records that fall within the scope of 5 U.S.C. 552a(k)(1), (k)(2), or (k)(5) may be exempt from the provisions of 5 U.S.C. 552a(c)(3), (d)(1) through (d)(5), (e)(1), (e)(4)(G), (e)(4)(H), and (e)(4)(I), and (f).

(iii) *Authority*: 5 U.S.C. 552a(k)(1), (k)(2), and (k)(5).

(iv) *Reasons*: (A) From subsection (c)(3) because disclosing the agencies to which information from this system has been released could reveal the subject's involvement in a sensitive intelligence or counterintelligence operation or investigation of an actual or potential criminal violation, or intelligence operation or investigation; or the existence of that investigation or operation. Granting access to such information could seriously impede or compromise an investigation or operation; endanger the physical safety of participants and their families, confidential sources, witnesses, intelligence personnel, and their families; and lead to the improper influencing of witnesses; the destruction of evidence or the fabrication of testimony and disclose investigative techniques and procedures.

(B) From subsection (d)(1) through (d)(5) because granting access to records could inform the subject of an intelligence or counterintelligence operation or investigation of an actual or potential criminal violation or the existence of that operation or investigation; of the nature and scope of the information and evidence obtained, or of the identity of confidential sources, witnesses and intelligence personnel. Granting access to such information could seriously impede or compromise an operation or investigation; endanger the physical safety of confidential sources, witnesses, intelligence personnel and their families; lead to the improper influencing of witnesses; the destruction of evidence or the fabrication of testimony; disclose investigative techniques and procedures; invade the privacy of those individuals involved in intelligence programs and their families; compromise and thus negate specialized techniques used to support intelligence programs; and interfere with and negate the orderly conduct of intelligence and counterintelligence operations and investigations. In addition, the agency is required to protect the confidentiality of sources who furnished information to the Government under an expressed promise of confidentiality or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. This confidentiality is needed to maintain the Government's continued access to information from persons who otherwise might refuse to give it.

(C) From subsection (e)(1) because it is not always possible to detect the relevance of specific information in the early stages of an investigation or operation. Relevance and necessity are often questions of judgment and timing, and it is only after the information is evaluated that the relevance and necessity of such information can be established. In addition, during the course of the investigation or operation, the investigator or operative may obtain information which is incidental to the main purpose of the investigative jurisdiction of another agency. Such information cannot readily be segregated. Furthermore, during the course of the investigation or oper-

ation, the investigator may obtain information concerning violations of law other than those which are within the scope of his/her jurisdiction. In the interest of effective intelligence operations and law enforcement, military intelligence agents should retain information, since it is an aid in establishing patterns of criminal or intelligence activity and provides valuable leads for other law enforcement or intelligence agencies.

(D) From subsection (e)(4)(G), (e)(4)(H), and (f) because this system or records is being exempt from subsections (d) of the Act, concerning access to records. These requirements are inapplicable to the extent that this system of records will be exempt from subsections (d)(1) through (d)(5) of the Act. Although the system would be exempt from these requirements, the Deputy Chief of Staff for Intelligence has published information concerning its notification, access, and contest procedures because under certain circumstances, the Deputy Chief of Staff for Intelligence could decide it is appropriate for an individual to have access to all or a portion of his/her records in this system of records.

(E) From subsection (e)(4)(I) because it is necessary to protect the confidentiality of sources of information, to protect the privacy and physical safety of participants and their families, confidential sources, and witnesses and to avoid the disclosure of specialized techniques and procedures. Although the system will be exempt from this requirement, the Deputy Chief of Staff for Intelligence has published such a notice in broad, generic terms.

(f) *Exempt OPM records.* Three Office of Personnel Management systems of records apply to Army employees, except for nonappropriated fund employees. These systems, the specific exemptions determined to be necessary and proper, the records exempted, provisions of the Privacy Act from which exempt, and justification are set forth below:

(1) *Personnel Investigations Records (OPM/CENTRAL-9).* All material and information in these records that meets the criteria stated in 5 U.S.C. 552a(k)(1), (k)(2), (k)(3), (k)(5), and (k)(6) is exempt from the requirements

of 5 U.S.C. 552a(c)(3) and (d). These provisions of the Privacy Act relate to making accountings of disclosures available to the data subject and access to and amendment of records. The specific applicability of the exemptions to this system and the reasons for the exemptions are as follows:

(i) Personnel investigations may obtain from another Federal agency properly classified information which pertains to national defense and foreign policy. Application of exemption (k)(1) may be necessary to preclude the data subject's access to and amendment of such classified information under 5 U.S.C. 552a(d).

(ii) Personnel investigations may contain investigatory material compiled for law enforcement purposes other than material within the scope of 5 U.S.C. 552a(j)(2), e.g., investigations into the administration of the merit system. Application of exemption (k)(2) may be necessary to preclude the data subject's access to or amendment of such records, under 552a(c)(3) and (d).

(iii) Personnel investigations may obtain from another Federal agency information that relates to providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18. Application of exemption (k)(3) may be necessary to preclude the data subject's access to and amendment of such records under 5 U.S.C. 552a(d).

(iv) All information about individuals in these records that meets the criteria stated in 5 U.S.C. 552a(k)(5) is exempt from the requirements of 5 U.S.C. 552a(c)(3) and (4). These provisions of the Privacy Act relate to making accountings of disclosures available to the data subject, and access to and amendment of records. These exemptions are claimed because this system contains investigatory material compiled solely for the purpose of determining suitability, eligibility, and qualifications for Federal civilian employment. To the extent that the disclosure of material would reveal the identity of source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to September 27, 1975, under an implied promise that the identity of

the source would be held in confidence, the application of exemption (k)(5) will be required to honor such a promise should the data subject request access to or amendment of the record, or access to the accounting of disclosures of the record.

(v) All material and information in the records that meets the criteria stated in 5 U.S.C. 552a(k)(6) is exempt from the requirements of 5 U.S.C. 552a(d), relating to access to and amendment of records by the data subject. This exemption is claimed because portions of this system relate to testing or examination materials used solely to determine individual qualifications for appointment or promotion in the Federal service. Access to or amendment of this information by the data subject would compromise the objectivity and fairness of the testing or exemption process.

*(2) Recruiting, Examining, and Placement Records (OPM/GOVT-5).*

(i) All information about individuals in these records that meets the criteria stated in 5 U.S.C. 552a(k)(5) is exempt from the requirements of 5 U.S.C. 552a(c)(3) and (d). These provisions of the Privacy Act relate to making accountings of disclosures available to the data subject and access to and amendment of records. These exemptions are claimed because this system contains investigative material compiled solely for the purpose of determining the appropriateness of a request for approval of an objection to an eligible's qualification for employment in the Federal service. To the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, the application of exemption (k)(5) will be required to honor such a promise should the data subject request access to the accounting of disclosures of the record.

(ii) All material and information in these records that meets the criteria stated in 5 U.S.C. 552a(k)(6) are exempt from the requirements of 5 U.S.C. 552a(d), relating to access to and amendment of records by the subject. The exemption is claimed because portions of this system relate to testing or

## Department of the Army, DoD

## Pt. 505, App. A

examination materials used solely to determine individual qualification for appointment or promotion in the Federal service and access to or amendment of this information by the data subject would compromise the objectivity and fairness of the testing or examining process.

(3) *Personnel Research Test Validation Records (OPM/GOVT-6)*. All material and information in these records that meets the criteria stated in 5 U.S.C. 552a(k)(6) is exempt from the requirements of 5 U.S.C. 552a(d), relating to access to and amendment of the records by the data subject. This exemption is claimed because portions of this system relate to testing or examination materials used solely to determine individual qualifications for appointment or promotion in the Federal service. Access to or amendment of this information by the data subject would compromise the objectivity and fairness of the testing or examination process.

[61 FR 43657, Aug. 26, 1996, as amended at 62 FR 48480, Sept. 16, 1997; 64 FR 45877, Aug. 23, 1999; 65 FR 6895, Feb. 11, 2000; 66 FR 55876, Nov. 5, 2001; 67 FR 17618, Apr. 11, 2002]

### APPENDIX A TO PART 505—EXAMPLE OF SYSTEM OF RECORDS NOTICE

#### *A0319.01DACA*

#### *System name:*

Out-of-Service Accounts Receivables.

#### *System location:*

US Army Finance and Accounting Center,  
Ft Benjamin Harrison, IN 46249.

#### *Categories of individuals covered by the system:*

Separated and retired military/civilian personnel and others indebted to the US Army.

#### *Categories of records in the system:*

Records of current and former military members and civilian employees' pay accounts showing entitlements, deductions, payments made, and any indebtedness resulting from deductions and payments exceeding entitlements. These records include, but are not limited to:

a. Individual military pay records, substantiating documents such as military pay orders, pay adjustment authorizations, military master pay account printouts from the Joint Uniform Military Pay System (JUMPS), records of travel payments, finan-

cial record data folders, miscellaneous vouchers, personal financial records, credit reports, promissory notes, individual financial statements, and correspondence;

b. Application for waiver of erroneous payments or for remission of indebtedness with supporting documents, including, but not limited to statements of financial status (personal income and expenses), statements of commanders and/or accounting and finance officers, correspondence with members and employees;

c. Claims of individuals requesting additional payments for service rendered with supporting documents including, but not limited to, time and attendance reports, leave and earnings statements, travel orders and/or vouchers, and correspondence with members and employees;

d. Delinquent accounts receivable from field accounting and finance officers including, but not limited to, returned checks, medical services billings, collection records, and summaries of the Army Criminal Investigations Command and/or Federal Bureau of Investigation reports;

e. Reports from probate courts regarding estates of deceased debtors;

f. Reports from bankruptcy courts regarding claims of the United States against debtors.

#### *Authority for maintenance of the system:*

31 U.S.C., section 3711; 10 U.S.C., section 2774; and 12 U.S.C., section 1715.

#### *Purpose:*

To process, monitor, and post-audit accounts receivable, to administer the Federal Claims Collection Act, and to answer inquiries pertaining thereto.

#### *Routine users of records maintained in the system, including categories of users and the purposes of such uses:*

Information may be disclosed to:

US Department of Justice/US Attorneys: For legal action and/or final disposition of the debt claims. The litigation briefs (comprehensive, written referral recommendations) will restructure the entire scope of the collection cases.

Internal Revenue Service: To obtain locator status for delinquent accounts receivables; (Automated controls exist to preclude redisclosure of solicited IRS address data); and/or to report write-off amounts as taxable income as pertains to amounts compromised and accounts barred from litigation due to age.

Private Collection Agencies: For collection action when the Army has exhausted its internal collection efforts.

**Pt. 505, App. B**

**32 CFR Ch. V (7-1-02 Edition)**

*Disclosure to Consumer Reporting Agencies:*

Disclosures pursuant to 5 U.S.C. 552a(b)(12) may be made to "consumer reporting agencies" as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f) or the Federal Claims Collection Act of 1966 (31 U.S.C. 3701(a)(3)) when an individual is responsible for a debt to the US Army, provided the debt has been validated, is overdue, and the debtor has been advised of the disclosure and his rights to dispute, appeal or review the claim; and/or whenever a financial status report is requested for use in the administration of the Federal Claims Collection Act. Claims of the United States may be compromised, terminated or suspended when warranted by information collected.

*Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:*

*Storage:*

Paper records in collection file folders and bulk storage; card files, computer magnetic tapes and printouts; microfiche.

*Retrievability:*

By Social Security Number, name, and substantiating document number; conventional indexing is used to retrieve data.

*Safeguards:*

The US Army Finance and Accounting Center employs security guards. An employee badge and visitor registration system is in effect. Hard copy records are maintained in areas accessible only to authorized personnel who are properly screened, cleared and trained. Computerized records are accessed by custodian of the records system and by persons responsible for servicing the record system in the performance of their official duties. Certifying finance and accounting officers of debts have access to debt information to confirm if the debt is valid and collection action is to be continued. Computer equipment and files are located in a separate secured area.

*Retention and disposal:*

Individual military pay records and accounts receivables are converted to microfiche and retained for 6 years. Destruction is by shredding. Retention periods for other records vary according to category, but total retention does not exceed 56 years; these records are sent to the Federal Records Center, General Services Administration at Dayton, Ohio; destruction is by burning or salvage as waste paper.

*System manager(s) and address:*

Commander, US Army Finance and Accounting Center Indianapolis, IN 46249.

*Notification procedure:*

Individuals desiring to know whether this system of records contains information about them should contact the System Manager, ATTN: FINCP-F, furnishing full name, Social Security Number, and military status or other information verifiable from the record itself.

*Record access procedures:*

Individuals seeking access to records in this system pertaining to them should submit a written request as indicated in "Notification procedure" and furnish information required therein.

*Contesting record procedures:*

The Army's rules for access to records and for contesting and appealing initial determinations are contained in Army Regulation 340-21 (32 CFR part 505).

*Record source categories:*

Information is received from Department of Defense staff and field installations, Social Security Administration, Treasury Department, financial organizations, and automated system interface.

*Systems exempted from certain provisions of the act:*

None.

**APPENDIX B TO PART 505—EXAMPLE OF REPORT FOR NEW SYSTEM OF RECORDS**

*Narrative Statement*

1. *System Identification and Name:* A0404.02DAJA, Courts-Martial Files.

2. *Responsible Official:* Mr. James D. Kemper, US Army Legal Services Agency, Office of The Judge Advocate General, Room 204B, Nassif Building, Falls Church, VA 22041.

3. *Purpose of the System:* Records of trial by court-martial are necessary for the purpose of legal review and final action in court-martial cases. After completion of appellate review, they protect each accused against a subsequent trial for the same offense(s).

4. *Authority for the System:* Title 10 U.S.C., Chapter 47, Section 865 states that, in the case of a general court-martial or when sentence that includes a bad conduct discharge is approved by the convening authority in a special court-martial, the record will be sent to The Judge Advocate General. All other special and summary court-martial records will be reviewed by a Judge Advocate.

5. *Number (or estimate) of individuals on whom records will be maintained:* Approximately 7,000,000.

6. *Information on First Amendment Activities:* The system contains no information on First Amendment activities per se; however, the system may include records of trial in which

## Department of the Army, DoD

## Pt. 505, App. C

the charged misconduct was an activity arguably protected by the First Amendment.

7. *Measures to Assure Information Accuracy:* In a trial by court-martial, the accused has a unique opportunity to assure that his record is accurate, relevant, timely, and complete as it is made. He has the right to be present at trial, to be represented by counsel in general and special courts-martial and to consult with counsel prior to a summary courts-martial to review and challenge all information before it is introduced into evidence, to cross-examine all witnesses against him, to present evidence in his behalf, and in general and special courts-martial, to review and comment upon the record of trial before the convening authority's action.

8. *Other Measures to Assure System Security:* As courts-martial records reflect criminal proceedings ordinarily open to the public, copies are normally releasable to the public pursuant to the Freedom of Information Act. However, access to the original records is limited to authorized individuals. Security measures consist of standard physical security devices and civilian and military guards.

9. *Relationship to State/Local Government Activities:* None.

10. *Supporting Documentation:* Proposed system notice and proposed exemption rule are at Encl 1 and 2 respectively.

### APPENDIX C TO PART 505—PROVISIONS OF THE PRIVACY ACT FROM WHICH A GENERAL OR SPECIFIC EXEMPTION MAY BE CLAIMED

Exemption		Section of the Privacy Act
(j)(2)	(k)(1-7)	
No	No	(b)(1) Disclosures within the Department of Defense.
No	No	(2) Disclosures to the public.
No	No	(3) Disclosures for a "Routine Use."
No	No	(4) Disclosures to the Bureau of Census.
No	No	(5) Disclosures for statistical research and reporting.
No	No	(6) Disclosures to the National Archives.
No	No	(7) Disclosures for law enforcement purposes.
No	No	(8) Disclosures under emergency circumstances.
No	No	(9) Disclosures to the Congress.
No	No	(10) Disclosures to the General Accounting Office.
No	No	(11) Disclosures pursuant to court orders.
No	No	(12) Disclosure to consumer reporting agencies.
No	No	(c)(1) Making disclosure accountings.
No	No	(2) Retaining disclosure accountings.
Yes	Yes	(c)(3) Making disclosure accounting available to the individual.

Exemption		Section of the Privacy Act
(j)(2)	(k)(1-7)	
Yes	No	(c)(4) Informing prior recipients of corrections.
Yes	Yes	(d)(1) Individual access to records.
Yes	Yes	(2) Amending records.
Yes	Yes	(3) Review of the Component's refusal to amend a record.
Yes	Yes	(4) Disclosure of disputed information.
Yes	Yes	(5) Access to information compiled in anticipation of civil action.
Yes	Yes	(e)(1) Restrictions on collecting information.
Yes	No	(e)(2) Collecting directly from the individual.
Yes	No	(3) Informing individuals from whom information is requested.
No	No	(e)(4)(A) Describing the name and location of the system.
No	No	(B) Describing categories of individuals.
No	No	(C) Describing categories of records.
No	No	(D) Describing routine uses.
No	No	(E) Describing records management policies and practices.
No	No	(F) Identifying responsible officials.
Yes	Yes	(e)(4)(G) Procedures for determining if a system contains a record on an individual.
Yes	Yes	(H) Procedures for gaining access.
Yes	Yes	(I) Describing categories of information sources.
Yes	No	(e)(5) Standards of accuracy.
No	No	(e)(6) Validating records before disclosure.
No	No	(e)(7) Records of First Amendment activities.
No	No	(e)(8) Notification of disclosure under compulsory legal process.
No	No	(e)(9) Rules of conduct.
No	No	(e)(10) Administrative, technical and physical safeguards.
No	No	(11) Notice for new and revised routine uses.
Yes	Yes	(f)(1) Rules for determining if an individual is subject of a record.
Yes	Yes	(f)(2) Rules for handling access requests.
Yes	Yes	(f)(3) Rules for granting access.
Yes	Yes	(f)(4) Rules for amending records.
Yes	Yes	(f)(5) Rules regarding fees.
Yes	No	(g)(1) Basis for civil action.
Yes	No	(g)(2) Basis for judicial review and remedies for refusal to amend.
Yes	No	(g)(3) Basis for judicial review and remedies for denial of access.
Yes	No	(g)(4) Basis for judicial review and remedies for other failure to comply.
Yes	No	(g)(5) Jurisdiction and time limits.
Yes	No	(h) Rights of legal guardians.
No	No	(i)(1) Criminal penalties for unauthorized disclosure.
No	No	(2) Criminal penalties for failure to publish.
No	No	(3) Criminal penalties for obtaining records under false pretenses.
Yes	No	(j) Rulemaking requirement.
N/A	No	(j)(1) General exemption for the Central Intelligence Agency.

**Pt. 505, App. D**

Exemption		Section of the Privacy Act
(j)(2)	(k)(1-7)	
N/A	No	(j)(2) General exemption for criminal law enforcement records.
Yes	N/A	(k)(1) Exemption for classified material.
N/A	N/A	(k)(2) Exemption for law enforcement material.
Yes	N/A	(k)(3) Exemption for records pertaining to Presidential protection.
Yes	N/A	(k)(4) Exemption for statistical records.
Yes	N/A	(k)(5) Exemption for investigatory material compiled for determining suitability for employment or service.
Yes	N/A	(k)(6) Exemption for testing or examination material.
Yes	N/A	(k)(7) Exemption for promotion evaluation materials used by the Armed Forces.
Yes	No	(l)(1) Records stored in GSA records centers.
Yes	No	(l)(2) Records archived before September 27, 1975.
Yes	No	(l)(3) Records archived on or after September 27, 1975.
Yes	No	(m) Applicability to government contractors.
Yes	No	(n) Mailing lists.
Yes	No	(o) Reports on new systems.
Yes	No	(p) Annual report.

**APPENDIX D TO PART 505—GLOSSARY OF TERMS**

**Section I**

**Abbreviations**

AAFES
Army and Air Force Exchange Service
AARA
Access and Amendment Refusal Authority
ACSIM
Assistant Chief of Staff for Information Management
DA
Department of the Army
DOD
Department of Defense
GAO
General Accounting Office
GSA
General Services Administration
JUMPS
Joint uniform military pay system
MACOM
Major Army command

**32 CFR Ch. V (7-1-02 Edition)**

MPMIS
Military Police management information system
NARS
National Archives and Records Service
NGB
National Guard Bureau
OMB
Office of Management and Budget
OPM
Office of Personnel Management
SSN
Social Security Number
TAG
The Adjutant General
TIG
The Inspector General
TJAG
The Judge Advocate General
USACIDC
U.S. Army Criminal Investigation Command

**Section II**

**Terms**

ACCESS
The review of a record or obtaining a copy of a record or parts thereof in a system of records.
AGENCY
The DOD is a single agency for the purpose of disclosing records subject to The Privacy Act of 1974. For other purposes, including access, amendment, appeals from denials of access or amendment, exempting systems of records, and record-keeping for release to non-DOD agencies, the DA is an agency.
ACCESS AND AMENDMENT REFUSAL AUTHORITY
The Army Staff agency head or major Army commander designated sole authority by this regulation to deny access to, or refuse amendment of, records in his or her assigned area or functional specialization.
CONFIDENTIAL SOURCE
A person or organization that has furnished information to the Federal Government under an express promise that its identity would be withheld, or under an implied promise of such confidentiality if this implied promise was made before September 27, 1975.

## Department of the Army, DoD

Pt. 507

### DATA SUBJECT

The individual about whom the Army is maintaining information in a system of records.

### DISCLOSURE

The furnishing of information about an individual by any means, to an organization, Government agency, or to an individual who is not the subject of the record, the subject's designated agent or legal guardian. Within the context of the Privacy Act and this regulation, this term applies only to personal information that is a part of a system of records.

### INDIVIDUAL

A living citizen of the United States or an alien admitted for permanent residence. The Privacy Act rights of an individual may be exercised by the parent or legal guardian of a minor or an incompetent. (The Privacy Act confers no rights on deceased persons, nor may their next-of-kin exercise any rights for them.)

### MAINTAIN

Collect, use, maintain, or disseminate.

### OFFICIAL USE

Any action by a member or employee of DOD that is prescribed or authorized by law or a regulation and is intended to perform a mission or function of the Department.

### PERSONAL INFORMATION

Information about an individual that is intimate or private to the individual, as distinguished from information related solely to the individual's official functions or public life.

### PRIVACY ACT REQUEST

A request from an individual for information about the existence of, or for access to or amendment of, a record about him or her that is in a system of records. The request must cite or implicitly refer to the Privacy Act.

### RECORD

Any item, collection, or grouping of information about an individual that—

a. Is kept by the Government including, but not limited to, an individual's home address, home telephone number, SSN, education, financial transactions, medical history, and criminal or employment history.

b. Contains an individual's name, identifying number, symbol, or other individual identifier such as a finger, voice print, or a photograph.

### ROUTINE USE

Disclosure of a record outside DOD without the consent of the subject individual for a use that is compatible with the purpose for which the information was collected and maintained by DA. The routine use must be included in the published system notice for the system of records involved.

### STATISTICAL RECORD

A record maintained only for statistical research or reporting purposes and not used in whole or in part in making determinations about specific individuals.

### SYSTEM MANAGER

The official responsible for policies and procedures for operating and safeguarding a system or records. This official is located normally at Headquarters, DA.

### SYSTEM OF RECORDS

A group of records under the control of DA from which information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to the individual. System notices for all systems of records must be published in the FEDERAL REGISTER. (A grouping or files series of records arranged chronologically or subjectively that is not retrieved by individual identifier is not a system of records, even though individual information could be retrieved by such an identifier, such as through a paper-by-paper search.)

## **PART 507—MANUFACTURE AND SALE OF DECORATIONS, MEDALS, BADGES, INSIGNIA, COMMERCIAL USE OF HERALDIC DESIGNS AND HERALDIC QUALITY CONTROL PROGRAM**

### **Subpart A—Introduction**

Sec.

507.1 Purpose.

507.2 References.

507.3 Explanation of abbreviations and terms.

507.4 Responsibilities.

507.5 Statutory authority.

### **Subpart B—Manufacture and Sale of Decorations, Medals, Badges, and Insignia**

507.6 Authority to manufacture.

507.7 Authority to sell.

507.8 Articles authorized for manufacture and sale.

507.9 Articles not authorized for manufacture or sale.